WIKIPEDIA 25
25 years of the free encyclopedia

Wi-Fi

Wi-Fi (/ˈwaɪfaɪ/)[1][a] is a family of wireless network protocols based on the IEEE 802.11 family of standards, which are commonly used for local area networking of devices and Internet access, allowing nearby digital devices to exchange data by radio waves. These are the most widely used computer networks, used globally in home and small office networks to link devices and to provide Internet access with wireless routers and wireless access points in public places such as coffee shops, restaurants, hotels, libraries, and airports.

Wi-Fi

Introduced	21 September 1997
Frequency	2.4, 5 and 6 GHz
Compatible hardware	Personal computers, video game consoles, smart devices, televisions, printers, security cameras

Wi-Fi is a trademark of the Wi-Fi Alliance, which restricts the use of the term "*Wi-Fi Certified*" to products that successfully complete interoperability certification testing.[3][4][5] Non-compliant hardware is simply referred to as WLAN, and it may or may not work with "*Wi-Fi Certified*" devices. As of 2017, the Wi-Fi Alliance consisted of more than 800 companies from around the world.[6] As of 2019, over 3.05 billion Wi-Fi-enabled devices are shipped globally each year.[7]

Wi-Fi uses multiple parts of the IEEE 802 protocol family and is designed to work well with its wired sibling, Ethernet. Compatible devices can network through wireless access points with each other as well as with wired devices and the Internet. Different versions of Wi-Fi are specified by various IEEE 802.11 protocol standards, with different radio technologies determining radio bands, maximum ranges, and speeds that may be achieved. Wi-Fi most commonly uses the 2.4 gigahertz (120 mm) UHF and 5 gigahertz (60 mm) SHF radio bands, with the 6 gigahertz SHF band used in newer generations of the standard; these bands are subdivided into multiple channels. Channels can be shared between networks, but, within range, only one transmitter can transmit on a channel at a time.

Wi-Fi's radio bands work best for line-of-sight use. Common obstructions, such as walls, pillars, home appliances, etc., may greatly reduce range, but this also helps minimize interference between different networks in crowded environments. The range of an access point is about 20 m (66 ft) indoors, while some access points claim up to a 150 m (490 ft) range outdoors. Hotspot coverage can be as small as a single room with walls that block radio waves or as large as many square kilometers using multiple overlapping access points with roaming permitted between them. Over time, the speed and spectral efficiency of Wi-Fi has increased. As of 2025, some versions of Wi-Fi, running on suitable hardware at close range, can achieve speeds of 23 Gbit/s (gigabit per second).[8]

History

TP-Link AX1500 Wi-Fi 6 router

A 1985 ruling by the U.S. Federal Communications Commission released parts of the ISM bands for unlicensed use for communications in the United States.[9] These frequency bands include the same 2.4 GHz bands used by equipment such as microwave ovens, and are thus subject to interference.[10]

In 1991 in the city of Nieuwegein in the Netherlands, the NCR Corporation and AT&T invented the precursor to 802.11,[11] intended for use in cashier systems, under the name WaveLAN. NCR's Vic Hayes, who held the chair of IEEE 802.11 for ten years, along with Bell Labs engineer Bruce Tuch, approached the Institute of Electrical and Electronics Engineers (IEEE) to create a standard and were involved in designing the initial 802.11b and 802.11a specifications within the IEEE.[12] They have both been subsequently inducted into the Wi-Fi NOW Hall of Fame.[13]

In 1989 in Australia, a team of scientists began working on wireless LAN technology.[14] A prototype test bed for a wireless local area network (WLAN) was developed in 1992 by a team of researchers from the Radiophysics Division of the CSIRO (Commonwealth Scientific and Industrial Research Organisation) in Australia, led by John O'Sullivan.[15] A patent for Wi-Fi was lodged by the CSIRO in 1992.[16]

The first version of the 802.11 protocol was released in 1997, and provided up to 2 Mbit/s link speeds. This was updated in 1999 with 802.11b to permit 11 Mbit/s link speeds.

In 1999, the Wi-Fi Alliance formed as a trade association to hold the Wi-Fi trademark under which most IEEE 802.11 products are sold.[17]

The major commercial breakthrough came with Apple Inc. adopting Wi-Fi for their iBook series of laptops in 1999.[11] It was the first mass consumer product to offer Wi-Fi network connectivity, which was then branded by Apple as AirPort.[18] This was in collaboration with the same group that helped create the standard: Vic Hayes, Bruce Tuch, Cees Links, Rich McGinn, and others from Lucent.[19][20]

In 2000, Radiata, a group of Australian scientists connected to the CSIRO, were the first to use the 802.11a standard on chips connected to a Wi-Fi network.[16]

Wi-Fi uses a large number of patents held by multiple different organizations.[21] Australia,[22] the United States[23] and the Netherlands[24] simultaneously claim the invention of Wi-Fi, and a consensus has not been reached globally.[25][26] In 2009, the Australian CSIRO was awarded $200 million after a patent settlement with 14 technology companies, with a further $220 million awarded in 2012 after legal proceedings with 23 companies.[27][28][29]

In 2016, the CSIRO's WLAN prototype test bed was chosen as Australia's contribution to the exhibition *A History of the World in 100 Objects* held in the National Museum of Australia.[15]

Etymology and terminology

Apple AirPort Extreme installed in an iBook G4

The name *Wi-Fi*, commercially used as early as August 1999,[30] was coined by the brand-consulting firm Interbrand. The Wi-Fi Alliance had hired Interbrand to create a name that was "a little catchier than 'IEEE 802.11b Direct Sequence'."[31][32] According to Phil Belanger, a founding member of the Wi-Fi Alliance, the term *Wi-Fi* was chosen from a list of ten names that Interbrand proposed.[31] Interbrand also created the Wi-Fi logo. The yin-yang Wi-Fi logo indicates the certification of a product for interoperability.[33] The name is often written as *WiFi*, *Wifi*, or *wifi*, but these are not approved by the Wi-Fi Alliance.

It is disputed whether the name *Wi-Fi* is short-form for 'Wireless Fidelity',[34] although the Wi-Fi Alliance did use the advertising slogan "The Standard for Wireless Fidelity" for a short time after the brand name was created,[31][35] referenced "the Wi-Fi (Wireless Fidelity) logo" in a white paper[33] and the Wi-Fi Alliance was also called the "Wireless Fidelity Alliance Inc." in some publications.[36] IEEE, a separate but related organization, has stated "WiFi is a short name for Wireless Fidelity" on their website.[37][38] The name *Wi-Fi* was partly chosen because it sounds similar to Hi-Fi, which consumers take to mean *high fidelity* or *high quality*. Interbrand hoped consumers would find the name catchy, and that they would assume this *wireless* protocol has high fidelity because of its name.[39]

Other technologies intended for fixed points, including Motorola Canopy, are usually called *fixed wireless*. Alternative wireless technologies include Zigbee, Z-Wave, Bluetooth and mobile phone standards.

To connect to a Wi-Fi LAN, a computer must be equipped with a wireless network interface controller. The combination of a computer and an interface controller is called a *station*. Stations are identified by one or more MAC addresses.

Wi-Fi nodes often operate in infrastructure mode in which all communications go through a base station. *Ad hoc mode* refers to devices communicating directly with each other, without communicating with an access point.

A service set is the set of all the devices associated with a particular Wi-Fi network. Devices in a service set need not be on the same wavebands or channels. A service set can be local, independent, extended, mesh, or a combination. Each service set has an associated identifier, a 32-byte service set identifier (SSID), which identifies the network. The SSID is configured within the devices that are part of the network. A basic service set (BSS) is a group of stations that share the same wireless channel, SSID, and other settings that have wirelessly connected, usually to the same access point.[40]:3.6 Each BSS is identified by a MAC address called the *BSSID*.

Certification

Wi-Fi certification logo

The IEEE does not test equipment for compliance with their standards. The Wi-Fi Alliance was formed in 1999 to establish and enforce standards for interoperability and backward compatibility, and to promote wireless local-area-network technology. The Wi-Fi Alliance enforces the use of the Wi-Fi brand to technologies based on the IEEE 802.11 standards from the IEEE. Manufacturers with membership in the Wi-Fi Alliance, whose products pass the certification process, gain the right to mark those products with the Wi-Fi logo. Specifically, the certification process requires conformance to the IEEE 802.11 radio standards, the WPA and WPA2 security standards, and the EAP authentication standard. Certification may optionally include tests of IEEE 802.11 draft standards, interaction with cellular-phone technology in converged devices, and features relating to security set-up, multimedia, and power-saving.[41]

Not every Wi-Fi device is submitted for certification. The lack of Wi-Fi certification does not necessarily imply that a device is incompatible with other Wi-Fi devices.[42] The Wi-Fi Alliance may or may not sanction derivative terms, such as Super Wi-Fi,[43] coined by the US Federal Communications Commission (FCC) to describe proposed networking in the UHF TV band in the US.[44]

Versions and generations

Equipment frequently supports multiple versions of Wi-Fi. To communicate, devices must use a common Wi-Fi version. The versions differ between the radio wavebands they operate on, the radio bandwidth they occupy, the maximum data rates they can support and other details. Some versions permit the use of multiple antennas, which permits greater speeds as well as reduced interference.

Wi-Fi and IEEE 802.11 generations

Gen.[45][46]	IEEE standard	Adopt.	Link rate (Mbit/s)	RF (GHz)		
				2.4	5	6
—	802.11	1997	1–2	✓		
	802.11b	1999	1–11	✓		
	802.11a		6–54		✓	
	802.11g	2003		✓		
Wi-Fi 4	802.11n	2009	6.5–600	✓	✓	
Wi-Fi 5	802.11ac	2013	6.5–6,933	[b]	✓	
Wi-Fi 6	802.11ax	2021	0.4–9,608	✓	✓	
Wi-Fi 6E				✓	✓	✓
Wi-Fi 7	802.11be	2024	0.4–23,059	✓	✓	✓
Wi-Fi 8[47][48][49]	802.11bn	TBA		✓	✓	✓

Historically, the equipment listed the versions of Wi-Fi supported using the name of the IEEE standards. In 2018, the Wi-Fi Alliance introduced simplified Wi-Fi generational numbering to indicate equipment that supports Wi-Fi 4 (802.11n), Wi-Fi 5 (802.11ac) and Wi-Fi 6 (802.11ax). These generations have a high degree of backward compatibility with previous versions. The alliance has stated that the generational level 4, 5, or 6 can be indicated in the user interface when connected, along with the signal strength.[50][51]

The most important standards affecting Wi-Fi are: 802.11a, 802.11b, 802.11g, 802.11n (**Wi-Fi 4**), 802.11h, 802.11i, 802.11-2007, 802.11–2012, 802.11ac (**Wi-Fi 5**),[51] 802.11ad, 802.11af, 802.11-2016, 802.11ah, 802.11ai, 802.11aj, 802.11aq, 802.11ax (**Wi-Fi 6**),[51] 802.11ay.

Uses

Internet

An example of a service set called *WiFi Wikipedia* consisting of two basic service sets. The clients automatically roam between the two BSSs without the user having to explicitly connect to the second network.

Wi-Fi technology may be used to provide local network and Internet access to devices that are within Wi-Fi range of one or more routers that are connected to the Internet. The coverage of one or more interconnected access points can extend from an area as small as a few rooms to as large as many square kilometres. Coverage in the larger area may require a group of access points with overlapping coverage. For example, public outdoor Wi-Fi technology has been used successfully in wireless mesh networks in London. An international example is Fon.

Wi-Fi provides services in private homes, businesses, as well as in public spaces. Wi-Fi hotspots may be set up either free of charge or commercially, often using a captive portal webpage for access. Organizations, enthusiasts, authorities and businesses, such as airports, hotels, and restaurants, often provide free or paid-use hotspots to attract customers, to provide services to promote business in selected areas. Routers often incorporate a digital subscriber line modem or a cable modem and a Wi-Fi access point, are frequently set up in homes and other buildings, to provide Internet access for the structure.

Similarly, battery-powered routers may include a mobile broadband modem and a Wi-Fi access point. When subscribed to a cellular data carrier, they allow nearby Wi-Fi stations to access the Internet. A number of smartphones have a built-in mobile hotspot capability of this sort, though carriers often disable the feature, or charge a separate fee to enable it. Standalone devices such as MiFi- and WiBro-branded devices provide the capability. Some laptops that have a cellular modem card can also act as mobile Internet Wi-Fi access points.

Multiple traditional university campuses in the developed world provide at least partial Wi-Fi coverage. Carnegie Mellon University built the first campus-wide wireless Internet network, called Wireless Andrew, at its Pittsburgh campus in 1993 before Wi-Fi branding existed.[52][53][54] A number of universities collaborate in providing Wi-Fi access to students and staff through the Eduroam international authentication infrastructure.

City-wide

In the early 2000s, multiple cities around the world announced plans to construct citywide Wi-Fi networks. There are a number of successful examples; in 2004, Mysore (Mysuru) became India's first Wi-Fi-enabled city. A company called WiFiyNet has set up hotspots in Mysore, covering the whole city and a few nearby villages.[55]

An outdoor Wi-Fi access point

In 2005, St. Cloud, Florida and Sunnyvale, California, became the first cities in the United States to offer citywide free Wi-Fi (from MetroFi).[56] Minneapolis has generated $1.2 million in profit annually for its provider.[57]

In May 2010, the then London mayor Boris Johnson pledged to have London-wide Wi-Fi by 2012.[58] Several boroughs including Westminster and Islington[59][60] already had extensive outdoor Wi-Fi coverage at that point.

New York City announced a city-wide campaign to convert old phone booths into digital kiosks in 2014. The project, titled LinkNYC, has created a network of kiosks that serve as public Wi-Fi hotspots, high-definition screens and landlines. Installation of the screens began in late 2015. The city government plans to implement more than seven thousand kiosks over time, eventually making LinkNYC the largest and fastest public, government-operated Wi-Fi network in the world.[61][62][63][64][65] The UK has planned a similar project across major cities of the country, with the project's first implementation in the London Borough of Camden.[66]

Officials in South Korea's capital Seoul were moving to provide free Internet access at more than 10,000 locations around the city, including outdoor public spaces, major streets, and densely populated residential areas. Seoul was planning to grant leases to KT, LG Telecom, and SK Telecom. The companies were supposed to invest $44 million in the project, which was to be completed in 2015.[67]

Geolocation

Wi-Fi positioning systems use known positions of Wi-Fi hotspots to identify a device's location.[68][69][70] It is used when GPS isn't suitable due to issues like signal interference or slow satellite acquisition.[71] This includes assisted GPS, urban hotspot databases, and indoor positioning systems.[72] Wi-Fi positioning relies on measuring signal strength (RSSI) and fingerprinting.[73][74][75][76] Parameters like SSID and MAC address are crucial for identifying access points. The accuracy depends on nearby access points in the database. Signal fluctuations can cause errors, which can be reduced with noise-filtering techniques. For low precision, integrating Wi-Fi data with geographical and time information has been proposed.[77][78]

The Wi-Fi RTT capability introduced in IEEE 802.11mc allows for positioning based on round trip time measurement, an improvement over the RSSI method.[79] The IEEE 802.11az standard promises further improvements in geolocation accuracy.[80][81]

Motion detection

Wi-Fi sensing is used in applications such as motion detection and gesture recognition.[82]

Operational principles

Wi-Fi stations communicate by sending each other data packets, blocks of data individually sent and delivered over radio on various channels. As with all radio, this is done by the modulation and demodulation of carrier waves. Different versions of Wi-Fi use different techniques, 802.11b uses direct-sequence spread spectrum on a single carrier, whereas 802.11a, Wi-Fi 4, 5 and 6 use orthogonal frequency-division multiplexing.[83][84]

Channels are used half duplex[85][86] and can be time-shared by multiple networks. Any packet sent by one computer is locally received by stations tuned to that channel, even if that information is intended for just one destination.[c] Stations typically ignore information not addressed to them.[d] The use of the same channel also means that the data bandwidth is shared, so for example, available throughput to each device is halved when two stations are actively transmitting.

As with other IEEE 802 LANs, stations come programmed with a globally unique 48-bit MAC address.[e] The MAC addresses are used to specify both the destination and the source of each data packet. On the reception of a transmission, the receiver uses the destination address to determine whether the transmission is relevant to the station or should be ignored.

A scheme known as carrier-sense multiple access with collision avoidance (CSMA/CA) governs the way stations share channels. With CSMA/CA stations attempt to avoid collisions by beginning transmission only after the channel is sensed to be idle,[87][88] but then transmit their packet data in its entirety. CSMA/CA cannot completely prevent collisions, as two stations may sense the channel to be idle at the same time and thus begin transmission simultaneously. A collision happens when a station receives signals from multiple stations on a channel at the same time. This corrupts the transmitted data and can require stations to re-transmit. The lost data and re-transmission reduces throughput, in some cases severely.

Waveband

The 802.11 standard provides several distinct radio frequency ranges for use in Wi-Fi communications: 900 MHz, 2.4 GHz, 3.6 GHz, 4.9 GHz, 5 GHz, 6 GHz and 60 GHz bands.[89][90][91] Each range is divided into a multitude of channels. In the standards, channels are numbered at 5 MHz spacing within a band (except in the 60 GHz band, where they are 2.16 GHz apart), and the number refers to the centre frequency of the channel. Although channels are numbered at 5 MHz spacing, transmitters generally occupy at least 20 MHz, and standards allow for neighbouring channels to be bonded together to form a wider channel for higher throughput.

Countries apply their own regulations to the allowable channels, allowed users and maximum power levels within these frequency ranges. 802.11b/g/n can use the 2.4 GHz band, operating in the United States under FCC Part 15 rules and regulations. In this frequency band, equipment may occasionally

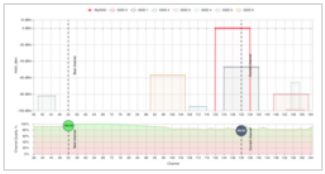
suffer interference from microwave ovens,[10] cordless telephones, USB 3.0 hubs,[92] Bluetooth and other devices.[93]

Spectrum assignments and operational limitations are not consistent worldwide: Australia and Europe allow for an additional two channels (12, 13) beyond the 11 permitted in the United States for the 2.4 GHz band, while Japan has three more (12–14).

802.11a/h/j/n/ac/ax can use the 5 GHz U-NII band, which, for much of the world, offers at least 23 non-overlapping 20 MHz channels. This is in contrast to the 2.4 GHz frequency band where the channels are only 5 MHz wide. In general, lower frequencies have longer range but have less capacity. The 5 GHz bands are absorbed to a greater degree by common building materials than the 2.4 GHz bands and usually give a shorter range.

As 802.11 specifications evolved to support higher throughput, the protocols have become much more efficient in their bandwidth use. Additionally, they have gained the ability to aggregate channels together to gain still more throughput where the bandwidth for additional channels is available. 802.11n allows for double radio spectrum bandwidth (40 MHz) per channel compared to 802.11a or 802.11g (20 MHz). 802.11n can be set to limit itself to 20 MHz bandwidth to prevent interference in dense communities.[94] In the 5 GHz band, 20 MHz, 40 MHz, 80 MHz, and 160 MHz channels are permitted with some restrictions, giving much faster connections.

An example of 2.4 GHz Wi-Fi spectrum

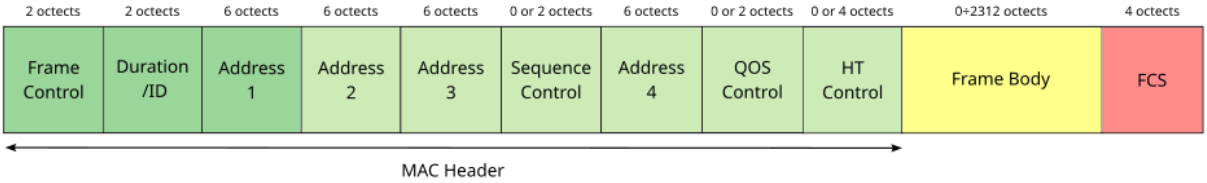


An example of 5 GHz Wi-Fi spectrum

This Netgear Wi-Fi router contains dual bands for transmitting the 802.11 standards across the 2.4 and 5 GHz spectrums and supports MIMO.

A dual-band cellular 4G+ Wi-Fi modem by Huawei

Communication stack



Wi-Fi is part of the IEEE 802 protocol family. The data is organized into 802.11 frames that are very similar to Ethernet frames at the data link layer, but with extra address fields. MAC addresses are used as network addresses for routing over the LAN.[95]

Wi-Fi's MAC and physical layer (PHY) specifications are defined by IEEE 802.11 for modulating and receiving one or more carrier waves to transmit the data in the infrared, and 2.4, 3.6, 5, 6, or 60 GHz frequency bands. They are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802). The base version of the standard was released in 1997 and has had many subsequent amendments. The standard and amendments provide the basis for wireless network products using the Wi-Fi brand. While each amendment is officially revoked when incorporated in the latest version of the standard, the corporate world tends to market to the revisions because they concisely denote capabilities of their products.[96] As a result, in the market place, each revision tends to become its own standard.

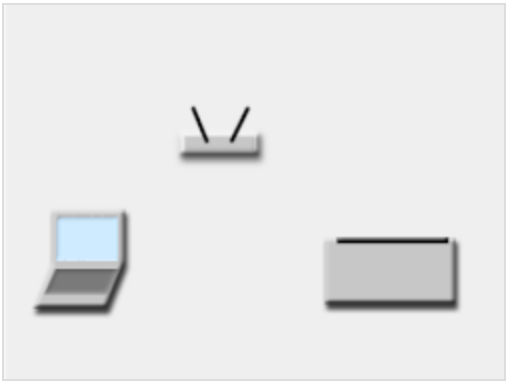
In addition to 802.11, the IEEE 802 protocol family has specific provisions for Wi-Fi. These are required because Ethernet's cable-based media are not usually shared, whereas with wireless all transmissions are received by all stations within the range that employ that radio channel. While Ethernet has essentially negligible error rates, wireless communication media are subject to significant interference. Therefore, the accurate transmission is not guaranteed so delivery is, therefore, a best-effort delivery mechanism. Because of this, for Wi-Fi, the Logical Link Control (LLC) specified by IEEE 802.2 employs Wi-Fi's media access control (MAC) protocols to manage retries without relying on higher levels of the protocol stack.[97]

For internetworking purposes, Wi-Fi is usually layered as a link layer[f] below the internet layer of the Internet Protocol. This means that nodes have an associated internet address and, with suitable connectivity, this allows full Internet access.

Modes

Infrastructure

In infrastructure mode, which is the most common mode used, all communications go through a base station. For communications within the network, this introduces an extra use of the airwaves but has the advantage that any two stations that can communicate with the base station can also communicate through the base station, which limits issues associated with the hidden node problem and simplifies the protocols.



A Wi-Fi network in infrastructure mode. The print job is sent from the computer via the AP to the printer.

Ad hoc and Wi-Fi direct

Wi-Fi also allows communications directly from one computer to another without an access point intermediary. This is called *ad hoc* Wi-Fi transmission. Different types of ad hoc networks exist. In the simplest case, network nodes must talk directly to each other. In more complex protocols nodes may forward packets, and nodes keep track of how to reach other nodes, even if they move around.

Ad hoc mode was first described by Chai Keong Toh in his 1996 patent of wireless ad hoc routing,[98] implemented on Lucent WaveLAN 802.11a wireless on IBM ThinkPads over a size nodes scenario spanning a region of over a mile. The success was recorded in *Mobile Computing* magazine (1999)[99] and later published formally in *IEEE Transactions on Wireless Communications*, 2002[100] and *ACM SIGMETRICS Performance Evaluation Review*, 2001.[101]

This wireless ad hoc network mode has proven popular with multiplayer video games on handheld game consoles, such as the Nintendo DS and PlayStation Portable. It is also popular on digital cameras, and other consumer electronics devices. Some devices can also share their Internet connection using ad hoc, becoming hotspots or virtual routers.[102]

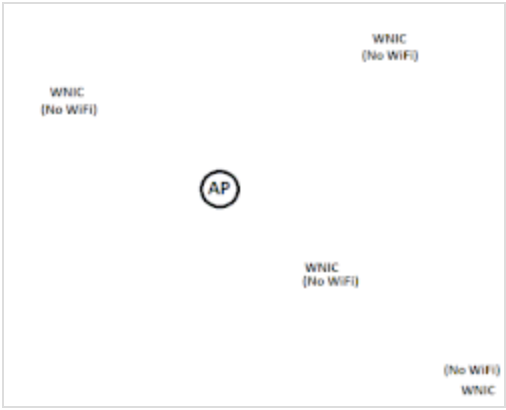
Similarly, the Wi-Fi Alliance promotes the specification Wi-Fi Direct for file transfers and media sharing through a new discovery and security methodology.[103] Wi-Fi Direct launched in October 2010.[104]

Another mode of direct communication over Wi-Fi is Tunneled Direct Link Setup (TDLS), which enables two devices on the same Wi-Fi network to communicate directly, instead of via the access point.[105]

Multiple access points

An Extended Service Set may be formed by deploying multiple access points that are configured with the same SSID and security settings. Wi-Fi client devices typically connect to the access point that can provide the strongest signal within that service set.[106]

Increasing the number of Wi-Fi access points for a network provides redundancy, better range, support for fast handover, and increased overall network capacity by using more channels or by defining smaller cells. Except for the smallest implementations (such as home or small office networks), Wi-Fi implementations have moved toward *thin* access points, with more of the network intelligence housed in a centralized network appliance, relegating individual access points to the role of dumb transceivers. Outdoor applications may use mesh topologies.[107]



Access points send out beacon frames to announce the presence of networks.

Performance

Wi-Fi operational range depends on factors such as the frequency band, modulation technique, transmitter power output, receiver sensitivity, antenna gain and type, and propagation and interference characteristics in the environment. At longer distances, speed is typically reduced.

Transmitter power

Compared to cell phones and similar technology, Wi-Fi transmitters are low-power devices. In general, the maximum amount of power that a Wi-Fi device can transmit is limited by local regulations, such as FCC Part 15 in the US. Equivalent isotropically radiated power (EIRP) in the European Union is limited to 20 dBm (100 mW).

Wi-Fi, however, has higher power compared to some other standards designed to support wireless personal area network applications. For example, Bluetooth provides a much shorter propagation range between 1 and 100 metres (1 and 100 yards)[108] and so in general has a lower power consumption. Other low-power technologies such as Zigbee have fairly long range, but much lower data rate. The high power consumption of Wi-Fi makes battery life in some mobile devices a concern.

Antenna

On wireless routers with detachable antennas, it is possible to improve range by fitting upgraded antennas. An access point compliant with either 802.11b or 802.11g, using the stock omnidirectional antenna might have a range of 0.1 km. The same radio with an external semi-parabolic antenna (15 dB gain) with a similarly equipped receiver at the far end might have a range of over 32 km.

Higher gain rating (dBi) indicates deviation from a theoretical, perfect isotropic radiator toward a directional antenna, and therefore the antenna can project or accept a usable signal further in particular directions, as compared to a similar output power on a more isotropic antenna.[109] For example, an 8 dBi antenna used with a 100 mW driver has a similar horizontal range to a 6 dBi antenna being driven at 500 mW. This assumes that radiation in the vertical direction is not useful for communications.

Parabolic dishes are directional and can give much greater range than omnidirectional antennas.

Yagi–Uda antennas, widely used for television reception, are relatively compact at Wi-Fi wavelengths.

Antenna of a Gigabyte GC-WB867D-I wireless network interface controller. Simple stick-like antennas have omnidirectional reception and relatively low range of 20 metres (yards) or so.

MIMO (multiple-input and multiple-output)

Wi-Fi 4 and higher standards allow devices to have multiple antennas on transmitters and receivers. Multiple antennas enable the equipment to exploit multipath propagation on the same frequency bands, giving higher speeds and more than doubled range.[110]

The Wi-Fi 5 standard uses the 5 GHz band exclusively, and is capable of multi-station WLAN throughput of at least 1 gigabit per second, and a single station throughput of at least 500 Mbit/s. This standard uses several signal processing techniques such as multi-user MIMO and 4×4 spatial multiplexing streams, and wide channel bandwidth (160 MHz) to achieve its gigabit throughput.

Radio propagation

With Wi-Fi signals, line-of-sight usually works best, but signals can absorb, reflect, refract, diffract and fade through and around structures, both man-made and natural. Wi-Fi signals are very strongly affected by metallic structures (including rebar in concrete, low-e coatings in glazing), rock structures (including marble) and water (such as found in vegetation).

Due to the complex nature of radio propagation at typical Wi-Fi frequencies, particularly around trees and buildings, algorithms can only approximately predict Wi-Fi signal strength for any given area in relation to a transmitter.[111] Performance associated with long-range Wi-Fi is more easily predicted, since longer links typically operate line-of-sight from towers that transmit above the surrounding foliage.

Distance records

Distance records (using non-standard devices) include 382 km (237 mi) in June 2007, held by Ermanno Pietrosemoli and EsLaRed of Venezuela, transferring about 3 MB/sec of data between the mountain-tops of El Águila and Platillon.[112] The Swedish National Space Agency transferred data 420 km (260 mi), using 6 watt amplifiers to reach an overhead stratospheric balloon.[113]

Interference

Wi-Fi connections can be blocked or the network throughput lowered by having other devices in the same area. Wi-Fi protocols are designed to share the radio bandwidth reasonably fairly. To minimize collisions with Wi-Fi and non-Wi-Fi devices, Wi-Fi employs Carrier-sense multiple access with collision avoidance (CSMA/CA), where transmitters listen before transmitting and delay transmission of packets if they detect that other devices are active on the channel, or if noise is detected from adjacent channels or non-Wi-Fi sources. Nevertheless, Wi-Fi networks are still susceptible to the hidden node and exposed node problems.[114]

A standard speed Wi-Fi signal occupies five channels in the 2.4 GHz band. Adjacent-channel interference can be caused by overlapping channels. Any two channel numbers that differ by five or more, such as 2 and 7, do not overlap. Channels 1, 6, and 11 are the only *group of three* non-overlapping channels in North America. However, whether the overlap is significant depends on physical spacing. Channels that differ by four interfere a negligible amount – much less than reusing

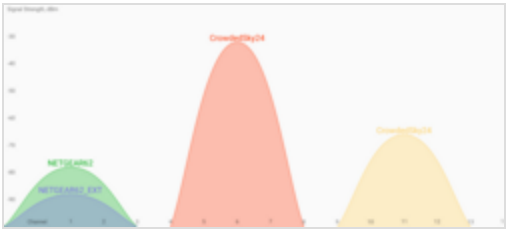
channels (which causes co-channel interference) – if transmitters are at least a few metres apart.[115] In Europe and Japan where channel 13 is available, using Channels 1, 5, 9, and 13 for 802.11g and 802.11n is viable and recommended.

However, multiple 2.4 GHz 802.11b and 802.11g access points default to the same channel on initial startup, contributing to congestion on certain channels. Wi-Fi pollution, or an excessive number of access points in the area, can prevent access and interfere with other devices' use of other access points, as well as decreasing overall signal-to-noise ratio (SNR). These issues can become a problem in high-density areas, such as large apartment complexes or office buildings with multiple Wi-Fi access points.[116] It is also an issue when municipalities[117] or other large entities (such as universities) seek to provide large area coverage.

Other devices use the 2.4 GHz band:[93] microwave ovens, ISM band devices, security cameras, Zigbee devices, Bluetooth devices, video senders, cordless phones, baby monitors,[118] and, in some countries, amateur radio, all of which can cause significant additional interference. On some 5 GHz bands interference from radar systems can occur in some places. Access points that support those bands employ dynamic frequency selection, which listens for radar, and if detected, will not permit transmission on that band.

Network planning frequency allocations for North America and Europe. Using these types of frequency allocations can help minimize co-channel and adjacent-channel interference.

These bands can be used by low-power transmitters without a licence, and with few restrictions. However, while unintended interference is common, users who have been found to cause deliberate interference (particularly for attempting to locally monopolize these bands for commercial purposes) have been issued large fines.[119]



In the 2.4 GHz wavebands as well as others, transmitters straddle multiple channels. Overlapping channels can suffer from interference unless this is a small portion of the total received power.

Throughput

Various layer-2 variants of IEEE 802.11 have different characteristics. Across all flavours of 802.11, maximum achievable throughputs are either given based on measurements under ideal conditions or in the layer-2 data rates. This, however, does not apply to typical deployments in which data are transferred between two endpoints, of which at least one is typically connected to a wired infrastructure. This means that typically data frames pass an 802.11 (WLAN) medium and are converted to 802.3 (Ethernet) or vice versa.

Due to the difference in the frame (header) lengths of these two media, the packet size of an application determines the speed of the data transfer. This means that an application that uses small packets (e.g., VoIP) creates a data flow with higher overhead and lower information rate.

Other factors that contribute to the overall application data rate include the energy with which the wireless signal is received. The latter is determined by distance and by the configured output power of the communicating devices.[120][121]

Hardware

Wi-Fi allows wireless deployment of local area networks (LANs). Also, spaces where cables cannot be run, such as outdoor areas and historical buildings, can host wireless LANs. However, building walls of certain materials, such as stone with high metal content, can block Wi-Fi signals.

A RouterBoard 112 with U.FL-RSMA antenna cable and R52 mini PCI Wi-Fi card, a setup widely used by wireless Internet service providers (WISPs) in the Czech Republic

A Wi-Fi device is a short-range wireless device. Wi-Fi devices are fabricated on RF CMOS integrated circuit (RF circuit) chips.[122]

Since the early 2000s, manufacturers are building wireless network adapters into most laptops. The price of chipsets for Wi-Fi continues to drop, making it an economical networking option included in ever more devices.[123]

Different competitive brands of access points and client network-interfaces can inter-operate at a basic level of service. Products designated as "Wi-Fi Certified" by the Wi-Fi Alliance are backward compatible. Unlike mobile phones, any standard Wi-Fi device works anywhere in the world.

An OSBRiDGE 3GN, an 802.11n access point and mobile broadband modem in one device

Access point

A wireless access point (WAP) connects a group of wireless devices to an adjacent wired LAN. An access point resembles a network hub, relaying data between connected wireless devices in addition to a (usually) single connected wired device, most often an Ethernet hub or switch, allowing wireless devices to communicate with other wired devices.

Wireless adapter

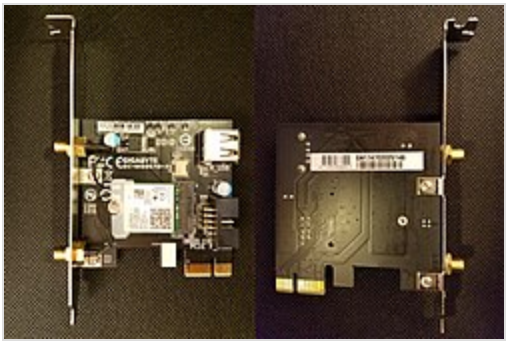
Wireless adapters allow devices to connect to a wireless network. These adapters connect to devices using various external or internal interconnects such as mini PCIe (mPCIe, M.2), USB, ExpressCard and previously PCI, Cardbus, and PC Card. As of 2010, most newer laptop computers come equipped with built-in internal adapters.

Router

An AirPort Wi-Fi adapter, supporting 802.11g, from an Apple MacBook

Wireless routers integrate a Wireless Access Point, Ethernet switch, and internal router firmware application that provides IP routing, NAT, and DNS forwarding through an integrated WAN-interface. A wireless router allows wired and wireless Ethernet LAN devices to connect to a (usually) single WAN device such as a cable modem, DSL modem, or optical modem. A wireless router allows all three devices, mainly the access point and router, to be configured through one central utility. This utility is usually an integrated web server that is accessible to wired and wireless LAN clients and often optionally to WAN clients. This utility may also be an application that is run on a computer, as is the case with as Apple's AirPort, which is managed with the AirPort Utility on macOS and iOS.[124]

Bridge



Wireless network interface controller Gigabyte GC-WB867D-I

Wireless network bridges can act to connect two networks to form a single network at the data-link layer over Wi-Fi. The main standard is the wireless distribution system (WDS).

Wireless bridging can connect a wired network to a wireless network. A bridge differs from an access point: an access point typically connects wireless devices to one wired network. Two wireless bridge devices may be used to connect two wired networks over a wireless link, useful in situations where a wired connection may be unavailable, such as between two separate homes or for devices that have no wireless networking capability (but have wired networking capability), such as consumer entertainment devices; alternatively, a wireless bridge can be used to enable a device that supports a wired connection to operate at a wireless networking standard that is faster than supported by the wireless network connectivity feature (external dongle or inbuilt) supported by the device (e.g., enabling Wireless-N speeds (up to the maximum supported speed on the wired Ethernet port on both the bridge and connected devices including the wireless access point) for a device that only supports Wireless-G). A dual-band wireless bridge can also be used to enable 5 GHz wireless network operation on a device that only supports 2.4 GHz wireless and has a wired Ethernet port.

Repeater

Wireless range-extenders or wireless repeaters can extend the range of an existing wireless network. Strategically placed range-extenders can elongate a signal area or allow for the signal area to reach around barriers such as those pertaining in L-shaped corridors. Wireless devices connected through repeaters suffer from an increased latency for each hop, and there may be a reduction in the maximum available data throughput. Besides, the effect of additional users using a network employing wireless range-extenders is to consume the available bandwidth faster than would be the case whereby a single user migrates around a network employing extenders. For this reason, wireless

range-extenders work best in networks supporting low traffic throughput requirements, such as for cases whereby a single user with a Wi-Fi-equipped tablet migrates around the combined extended and non-extended portions of the total connected network. Also, a wireless device connected to any of the repeaters in the chain has data throughput limited by the "weakest link" in the chain between the connection origin and connection end. Networks using wireless extenders are more prone to degradation from interference from neighbouring access points that border portions of the extended network and that happen to occupy the same channel as the extended network.

Embedded systems

The security standard, Wi-Fi Protected Setup, allows embedded devices with a limited graphical user interface to connect to the Internet with ease. Wi-Fi Protected Setup has 2 configurations: The Push Button configuration and the PIN configuration. These embedded devices are also called The Internet of things and are low-power, battery-operated embedded systems. Several Wi-Fi manufacturers design chips and modules for embedded Wi-Fi, such as GainSpan.[125]

Embedded serial-to-Wi-Fi module

Increasingly in the last few years (particularly as of 2007), embedded Wi-Fi modules have become available that incorporate a real-time operating system and provide a simple means of wirelessly enabling any device that can communicate via a serial port.[126] This allows the design of simple monitoring devices. An example is a portable ECG device monitoring a patient at home. This Wi-Fi-enabled device can communicate via the Internet.[127]

These Wi-Fi modules are designed by OEMs so that implementers need only minimal Wi-Fi knowledge to provide Wi-Fi connectivity for their products.

In June 2014, Texas Instruments introduced the first ARM Cortex-M4 microcontroller with an onboard dedicated Wi-Fi MCU, the SimpleLink CC3200. It makes embedded systems with Wi-Fi connectivity possible to build as single-chip devices, which reduces their cost and minimum size, making it more practical to build wireless-networked controllers into inexpensive ordinary objects.[128]

Security

The main issue with wireless network security is its simplified access to the network compared to traditional wired networks such as Ethernet. With wired networking, one must either gain access to a building (physically connecting into the internal network), or break through an external firewall. To access Wi-Fi, one must merely be within the range of the Wi-Fi network. Most business networks protect sensitive data and systems by attempting to disallow external access. Enabling wireless connectivity reduces security if the network uses inadequate or no encryption.[129][130][131]

An attacker who has gained access to a Wi-Fi network router can initiate a DNS spoofing attack against any other user of the network by forging a response before the queried DNS server has a chance to reply.[132]

Securing methods

A common measure to deter unauthorized users involves hiding the access point's name by disabling the SSID broadcast. While effective against the casual user, it is ineffective as a security method because the SSID is broadcast in the clear in response to a client SSID query. Another method is to only allow computers with known MAC addresses to join the network,[133] but determined eavesdroppers may be able to join the network by spoofing an authorized address.

Wired Equivalent Privacy (WEP) encryption was designed to protect against casual snooping but it is no longer considered secure. Tools such as AirSnort or Aircrack-ng can quickly recover WEP encryption keys.[134] Because of WEP's weakness the Wi-Fi Alliance approved Wi-Fi Protected Access (WPA) which uses TKIP. WPA was specifically designed to work with older equipment usually through a firmware upgrade. Though more secure than WEP, WPA has known vulnerabilities.

The more secure WPA2 using Advanced Encryption Standard was introduced in 2004 and is supported by most new Wi-Fi devices. WPA2 is fully compatible with WPA.[135] In 2017, a flaw in the WPA2 protocol was discovered, allowing a key replay attack, known as KRACK.[136][137]

A flaw in a feature added to Wi-Fi in 2007, called Wi-Fi Protected Setup (WPS), let WPA and WPA2 security be bypassed. The only remedy as of 2011 was to turn off Wi-Fi Protected Setup,[138] which is not always possible.

Virtual private networks can be used to improve the confidentiality of data carried through Wi-Fi networks, especially public Wi-Fi networks.[139]

A URI using the Wi-Fi scheme can specify the SSID, encryption type, password/passphrase, and if the SSID is hidden or not, so users can follow links from QR codes, for instance, to join networks without having to manually enter the data.[140] A MeCard-like format is supported by Android and iOS 11+.[141]

A QR code to automate a Wi-Fi connection, encoding the information *WIFI:S:Wikipedia;T:WPA;P:Password1!;;*

- Common format: `WIFI:S:<SSID>;T:<WEP|WPA|blank>;P:<PASSWORD>;H:<true|false|blank>;`
- Sample `WIFI:S:MySSID;T:WPA;P:MyPassW0rd;;`

Data security risks

Wi-Fi access points typically default to an encryption-free (*open*) mode. Novice users benefit from a zero-configuration device that works out-of-the-box, but this default does not enable any wireless security, providing open wireless access to a LAN. To turn security on requires the user to configure the device, usually via a software graphical user interface (GUI). On unencrypted Wi-Fi networks

connecting devices can monitor and record data (including personal information). Such networks can only be secured by using other means of protection, such as a VPN, or Hypertext Transfer Protocol over Transport Layer Security (HTTPS).

The older wireless-encryption standard, Wired Equivalent Privacy (WEP), has been shown easily breakable even when correctly configured. Wi-Fi Protected Access (WPA) encryption, which became available in devices in 2003, aimed to solve this problem. Wi-Fi Protected Access 2 (WPA2) ratified in 2004 is considered secure, provided a strong passphrase is used. The 2003 version of WPA has not been considered secure since it was superseded by WPA2 in 2004.

In 2018, WPA3 was announced as a replacement for WPA2, increasing security;[142] it rolled out on 26 June.[143]

Piggybacking

Piggybacking refers to access to a wireless Internet connection by bringing one's computer within the range of another's wireless connection, and using that service without the subscriber's explicit permission or knowledge.

During the early popular adoption of 802.11, providing open access points for anyone within range to use was encouraged to cultivate wireless community networks,[144] particularly since people on average use only a fraction of their downstream bandwidth at any given time.

Recreational logging and mapping of other people's access points have become known as wardriving. Indeed, many access points are intentionally installed without security turned on so that they can be used as a free service. Providing access to one's Internet connection in this fashion may breach the Terms of Service or contract with the Internet service provider (ISP). These activities do not result in sanctions in most jurisdictions; however, legislation and case law differ considerably across the world. A proposal to leave graffiti describing available services was called warchalking.[145]

Piggybacking often occurs unintentionally – a technically unfamiliar user might not change the default "unsecured" settings to their access point and operating systems can be configured to connect automatically to any available wireless network. A user who happens to start up a laptop in the vicinity of an access point may find the computer has joined the network without any visible indication. Moreover, a user intending to join one network may instead end up on another one if the latter has a stronger signal. In combination with automatic discovery of other network resources (see DHCP and Zeroconf) this could lead wireless users to send sensitive data to the wrong middle-man when seeking a destination (see man-in-the-middle attack). For example, a user could inadvertently use an unsecured network to log into a website, thereby making the login credentials available to anyone listening, if the website uses an insecure protocol such as plain HTTP without TLS.

On an unsecured access point, an unauthorized user can obtain security information (factory preset passphrase or Wi-Fi Protected Setup PIN) from a label on a wireless access point and use this information (or connect by the Wi-Fi Protected Setup pushbutton method) to commit unauthorized or unlawful activities.

Societal aspects

Wireless Internet access has become much more embedded in society. It has thus changed how the society functions in a number of ways.

Influence on developing countries

As of 2017 over half the world did not have access to the Internet,[78] prominently rural areas in developing nations. Technology that has been implemented in more developed nations is often costly and energy inefficient. This has led to developing nations using more low-tech networks, frequently implementing renewable power sources that can solely be maintained through solar power, creating a network that is resistant to disruptions such as power outages. For instance, in 2007, a 450-kilometre (280 mi) network between Cabo Pantoja and Iquitos in Peru was erected in which all equipment is powered only by solar panels.[78] These long-range Wi-Fi networks have two main uses: offer Internet access to populations in isolated villages, and to provide healthcare to isolated communities. In the case of the latter example, it connects the central hospital in Iquitos to 15 medical outposts which are intended for remote diagnosis.[78]

Work habits

Access to Wi-Fi in public spaces such as cafés or parks allows people, in particular freelancers, to work remotely. While the accessibility of Wi-Fi is the strongest factor when choosing a place to work (75% of people would choose a place that provides Wi-Fi over one that does not),[73] other factors influence the choice of specific hotspots. These vary from the accessibility of other resources, like books, the location of the workplace, and the social aspect of meeting other people in the same place. Moreover, the increase of people working from public places results in more customers for local businesses thus providing an economic stimulus to the area.

Additionally, in the same study it has been noted that wireless connection provides more freedom of movement while working. Both when working at home or from the office it allows the displacement between different rooms or areas. In some offices (notably Cisco offices in New York) the employees do not have assigned desks but can work from any office connecting their laptop to Wi-Fi hotspot.[73]

Housing

The Internet has become an integral part of living. As of 2016, 81.9% of American households have Internet access.[146] Additionally, 89% of American households with broadband connect via wireless technologies.[147] 72.9% of American households have Wi-Fi.

Wi-Fi networks have also affected how the interior of homes and hotels are arranged. For instance, architects have described that their clients no longer wanted only one room as their home office, but would like to work near the fireplace or have the possibility to work in different rooms. This contradicts architect's pre-existing ideas of the use of rooms that they designed. Additionally, some hotels have noted that guests prefer to stay in certain rooms since they receive a stronger Wi-Fi signal.[73]

Health concerns

The World Health Organization (WHO) says, "no health effects are expected from exposure to RF fields from base stations and wireless networks", but notes that they promote research into effects from other RF sources.[148] Although the WHO's International Agency for Research on Cancer (IARC) later classified radio-frequency electromagnetic fields (EMFs) as "possibly carcinogenic to humans (Group 2B)"[149] (a category used when "a causal association is considered credible, but when chance, bias or confounding cannot be ruled out with reasonable confidence"),[150] this classification was based on risks associated with wireless phone use rather than Wi-Fi networks.

The United Kingdom's Health Protection Agency reported in 2007 that exposure to Wi-Fi for a year results in the "same amount of radiation from a 20-minute mobile phone call".[151]

A review of studies involving 725 people who claimed electromagnetic hypersensitivity, "...suggests that 'electromagnetic hypersensitivity' is unrelated to the presence of an EMF, although more research into this phenomenon is required."[152]

Alternatives

Several other wireless technologies provide alternatives to Wi-Fi for different use cases:

- Bluetooth Low Energy, a low-power variant of Bluetooth
- Bluetooth, a short-distance network
- Cellular networks, used by smartphones
- LoRa, for long range wireless with low data rate
- NearLink, a short-range wireless technology standard
- WiMAX, for providing long range wireless internet connectivity
- Zigbee, a low-power, low data rate, short-distance communication protocol

Some alternatives are "no new wires", re-using existing cable:

- G.hn, which uses existing home wiring, such as phone and power lines

Several *wired* technologies for computer networking, which provide viable alternatives to Wi-Fi:

- Ethernet over twisted pair

See also

- Gi-Fi – a term used by some trade press to refer to faster versions of the IEEE 802.11 standards
- HiperLAN
- High-speed multimedia radio
- Indoor positioning system
- Li-Fi
- List of WLAN channels

- Operating system Wi-Fi support
- Passive Wi-Fi
- Power-line communication
- San Francisco Digital Inclusion Strategy
- WAPI
- WiGig
- Wireless Broadband Alliance
- Wi-Fi Direct

Explanatory notes

a. According to a founding member of the Wi-Fi Alliance, "Wi-Fi" has no expanded meaning, and was simply chosen as a more memorable name for the technology. Some Wi-Fi Alliance materials produced soon after this selection used the phrase *wireless fidelity*, but this was quickly dropped.[2]
b. 802.11ac only specifies operation in the 5 GHz band. Operation in the 2.4 GHz band is specified by 802.11n.
c. This *one speaks, all listen* property is a security weakness of shared-medium Wi-Fi since a node on a Wi-Fi network can eavesdrop on all traffic on the wire if it so chooses.
d. Unless it is put into promiscuous mode.
e. In some cases, the factory-assigned address can be overridden, either to avoid an address change when an adapter is replaced or to use locally administered addresses.
f. The link layer is equivalent to the physical and data link layers of the OSI model.

References

1. Garber, Megan (23 June 2014). " 'Why-Fi' or 'Wiffy'? How Americans Pronounce Common Tech Terms" (https://www.theatlantic.com/technology/archive/2014/06/why-fi-or-wiffy-how-americans-pronounce-techs-most-common-terms/373082/). *The Atlantic*. Archived (https://web.archive.org/web/20180615190651/https://www.theatlantic.com/technology/archive/2014/06/why-fi-or-wiffy-how-americans-pronounce-techs-most-common-terms/373082/) from the original on 15 June 2018.
2. "What Does Wi-Fi Stand For?" (https://www.newscientist.com/question/what-does-wi-fi-stand-for/). *New Scientist*. Archived (https://web.archive.org/web/20220105184518/https://www.newscientist.com/question/what-does-wi-fi-stand-for/) from the original on 5 January 2022. Retrieved 7 January 2022.
3. Beal, Vangie (2 May 2001). "What is Wi-Fi (IEEE 802.11x)? A Webopedia Definition" (http://www.webopedia.com/TERM/W/Wi_Fi.html). *Webopedia*. Archived (https://web.archive.org/web/20120308123721/http://www.webopedia.com/term/w/wi_fi.html) from the original on 8 March 2012.
4. Schofield, Jack (21 May 2007). "The Dangers of Wi-Fi Radiation (Updated)" (https://www.theguardian.com/technology/blog/2007/may/21/thedangersof). *The Guardian*. Archived (https://web.archive.org/web/20191101204649/https://www.theguardian.com/technology/blog/2007/may/21/thedangersof) from the original on 1 November 2019. Retrieved 1 November 2019 – via TheGuardian.com.
5. "Certification" (https://www.wi-fi.org/certification). *Wi-Fi.org*. Wi-Fi Alliance. Archived (https://web.archive.org/web/20200513210825/https://wi-fi.org/certification) from the original on 13 May 2020. Retrieved 1 November 2019.

6. "History | Wi-Fi Alliance" (https://www.wi-fi.org/who-we-are/history). *Wi-Fi Alliance*. Archived (https://web.archive.org/web/20171024205733/https://www.wi-fi.org/who-we-are/history) from the original on 24 October 2017. Retrieved 15 September 2020.
7. "Global Wi-Fi Enabled Devices Shipment Forecast, 2020 – 2024" (https://www.researchandmarkets.com/reports/5135535/global-wi-fi-enabled-devices-shipment-forecast). *Research and Markets*. 1 July 2020. Archived (https://web.archive.org/web/20210315203540/https://www.researchandmarkets.com/reports/5135535/global-wi-fi-enabled-devices-shipment-forecast) from the original on 15 March 2021. Retrieved 23 November 2020.
8. Weatherbed, Jess (13 October 2025). "Wi-Fi 8 demonstrated with first prototype connection" (https://www.theverge.com/news/798780/wi-fi-8-prototype-tp-link-test-explained). *The Verge*. Retrieved 2 January 2026.
9. "Authorization of Spread Spectrum Systems Under Parts 15 and 90 of the FCC Rules and Regulations" (https://web.archive.org/web/20070928054826/http://www.marcus-spectrum.com/documents/81413RO.txt). Federal Communications Commission of the USA. 18 June 1985. Archived from the original (http://www.marcus-spectrum.com/documents/81413RO.txt) (txt) on 28 September 2007. Retrieved 31 August 2007.
10. "Do Microwaves Interfere With WiFi Signals?" (https://www.scienceabc.com/innovation/do-microwaves-interfere-with-wifi-signals.html). 17 January 2018. Archived (https://web.archive.org/web/20220816204740/https://www.scienceabc.com/innovation/do-microwaves-interfere-with-wifi-signals.html) from the original on 16 August 2022. Retrieved 16 August 2022.
11. Claus Hetting (19 August 2018). "How a 1998 meeting with Steve Jobs gave birth to Wi-Fi" (https://wifinowglobal.com/news-and-blog/how-a-meeting-with-steve-jobs-in-1998-gave-birth-to-wi-fi/). *Wi-Fi NOW Global*. Archived (https://web.archive.org/web/20201215231732/https://wifinowglobal.com/news-and-blog/how-a-meeting-with-steve-jobs-in-1998-gave-birth-to-wi-fi/) from the original on 15 December 2020. Retrieved 27 May 2021.
12. Ben Charny (6 December 2002). "Vic Hayes – Wireless Vision" (https://web.archive.org/web/20120826164642/http://news.cnet.com/1200-1070-975460.html). *CNET*. Archived from the original (https://news.cnet.com/1200-1070-975460.html) on 26 August 2012. Retrieved 30 April 2011.
13. Hetting, Claus (8 November 2019). "Vic Hayes & Bruce Tuch inducted into the Wi-Fi Now Hall of Fame" (https://wifinowglobal.com/news-and-blog/vic-hayes-bruce-tuch-inducted-into-the-wi-fi-now-hall-of-fame/). *Wi-Fi Now Global*. Archived (https://web.archive.org/web/20201207194505/https://wifinowglobal.com/news-and-blog/vic-hayes-bruce-tuch-inducted-into-the-wi-fi-now-hall-of-fame/) from the original on 7 December 2020. Retrieved 27 November 2020.
14. Rimmer, Matthew. "CSIRO wins Wi-Fi patent litigation" (https://eprints.qut.edu.au/215127/). *QUT ePrints*.
15. Sibthorpe, Clare (4 August 2016). "CSIRO Wi-Fi invention to feature in upcoming exhibition at National Museum of Australia" (https://www.canberratimes.com.au/national/act/csiro-wifi-invention-to-feature-in-upcoming-exhibition-at-national-museum-of-australia-20160803-gqjyuv.html). *The Canberra Times*. Archived (https://web.archive.org/web/20160809200721/http://www.canberratimes.com.au/act-news/csiro-wifi-invention-to-feature-in-upcoming-exhibition-at-national-museum-of-australia-20160803-gqjyuv.html) from the original on 9 August 2016. Retrieved 4 August 2016.
16. O'Sullivan, John (8 February 2018). "How we made the wireless network". *Nature Electronics*. **1** (2): 147. doi:10.1038/s41928-018-0027-y (https://doi.org/10.1038%2Fs41928-018-0027-y).
17. "Wi-Fi Alliance: Organization" (https://www.wi-fi.org/organization.php). Official industry association Web site. Archived (https://web.archive.org/web/20090903004711/http://www.wi-fi.org/organization.php) from the original on 3 September 2009. Retrieved 23 August 2011.
18. "A brief history of Wi-Fi" (https://www.economist.com/technology-quarterly/2004/06/12/a-brief-history-of-wi-fi). *The Economist*. 12 July 2004. Archived (https://web.archive.org/web/20230102075107/https://www.economist.com/technology-quarterly/2004/06/12/a-brief-history-of-wi-fi) from the original on 2 January 2023. Retrieved 2 January 2023. "in July 1999 Apple introduced Wi-Fi as an option on its new iBook computers, under the brand name AirPort"

19. Steve Lohr (22 July 1999). "Apple Offers iMac's Laptop Offspring, the iBook" (https://www.nytimes.com/1999/07/22/business/apple-offers-imac-s-laptop-offspring-the-ibook.html). *The New York Times*. Archived (https://web.archive.org/web/20170202003816/http://www.nytimes.com/1999/07/22/business/apple-offers-imac-s-laptop-offspring-the-ibook.html) from the original on 2 February 2017. Retrieved 28 November 2020.
20. Lewis, Peter H. (25 November 1999). "State of the Art; Not Born To Be Wired" (https://www.nytimes.com/1999/11/25/technology/state-of-the-art-not-born-to-be-wired.html?pagewanted=all). *The New York Times*. Archived (https://web.archive.org/web/20170202002735/http://www.nytimes.com/1999/11/25/technology/state-of-the-art-not-born-to-be-wired.html?pagewanted=all) from the original on 2 February 2017. Retrieved 28 November 2020.
21. "IEEE SA – Records of IEEE Standards-Related Patent Letters of Assurance" (https://standards.ieee.org/about/sasb/patcom/patents/). *IEEE*. Archived (https://web.archive.org/web/20120410074816/http://standards.ieee.org/about/sasb/patcom/pat802_11.html) from the original on 10 April 2012.
22. "World changing Aussie inventions" (https://web.archive.org/web/20111215082408/http://www.australiangeographic.com.au/journal/world-changing-aussie-inventions.htm). *Australian Geographic*. Archived from the original (http://www.australiangeographic.com.au/journal/world-changing-aussie-inventions.htm) on 15 December 2011.
23. Field, Shivaune. "Hedy Lamarr: The Incredible Mind Behind Secure WiFi, GPS And Bluetooth" (https://web.archive.org/web/20230419123256/https://www.forbes.com/sites/shivaunefield/2018/02/28/hedy-lamarr-the-incredible-mind-behind-secure-wi-fi-gps-bluetooth/?sh=5871237541b7). *forbes.com*. Archived from the original (https://www.forbes.com/sites/shivaunefield/2018/02/28/hedy-lamarr-the-incredible-mind-behind-secure-wi-fi-gps-bluetooth/?sh=5871237541b7) on 19 April 2023. Retrieved 19 April 2023.
24. Van Der Meer, Hilde (26 March 2018). "10 Inventions You Didn't Know Were Dutch" (https://web.archive.org/web/20230419124142/https://investinholland.com/news/10-inventions-didnt-know-dutch/). *investinholland.com*. Netherlands Foreign Investment Agency. Archived from the original (https://investinholland.com/news/10-inventions-didnt-know-dutch/) on 19 April 2023. Retrieved 19 April 2023.
25. Mullin, Joe (4 April 2012). "How the Aussie government "invented WiFi" and sued its way to $430 million" (https://arstechnica.com/tech-policy/news/2012/04/how-the-aussie-government-invented-wifi-and-sued-its-way-to-430-million.ars). *Ars Technica*. Archived (https://web.archive.org/web/20120508201202/http://arstechnica.com/tech-policy/news/2012/04/how-the-aussie-government-invented-wifi-and-sued-its-way-to-430-million.ars) from the original on 8 May 2012.
26. Popper, Ben (3 June 2010). "Australia's Biggest Patent Troll Goes After AT&T, Verizon and T-Mobile" (https://www.cbsnews.com/news/australias-biggest-patent-troll-goes-after-at038t-verizon-and-t-mobile/). *CBS News*. Archived (https://web.archive.org/web/20130506135649/http://www.cbsnews.com/8301-505124_162-43340647/australias-biggest-patent-troll-goes-after-at038t-verizon-and-t-mobile/) from the original on 6 May 2013.
27. Brodkin, Jon (31 March 2012). "WiFi patent case results in $229 million payment to Australian government" (https://web.archive.org/web/20230419131311/https://arstechnica.com/tech-policy/2012/04/wifi-patent-case-results-in-229m-payment-to-australian-government/). *Ars Technica*. Archived from the original (https://arstechnica.com/tech-policy/2012/04/wifi-patent-case-results-in-229m-payment-to-australian-government/) on 19 April 2023. Retrieved 19 April 2023.
28. Schubert, Misha (31 March 2012). "Australian scientists cash in on Wi-Fi invention" (https://www.smh.com.au/technology/australian-scientists-cash-in-on-wifi-invention-20120331-1w5gx.html). *The Sydney Morning Herald*. Archived (https://web.archive.org/web/20120401162238/http://www.smh.com.au/it-pro/government-it/australian-scientists-cash-in-on-wifi-invention-20120331-1w5gx.html) from the original on 1 April 2012.
29. "CSIRO wins legal battle over wi-fi patent" (https://www.abc.net.au/news/2012-04-01/csiro-receives-payment-for-wifi-technology/3925814). *ABC News*. 1 April 2012. Archived (https://web.archive.org/web/20190807090636/https://www.abc.net.au/news/2012-04-01/csiro-receives-payment-for-wifi-technology/3925814) from the original on 7 August 2019. Retrieved 27 February 2019.

30. "Statement of Use, s/n 75799629, US Patent and Trademark Office Trademark Status and Document Retrieval" (http://tsdr.uspto.gov/documentviewer?caseId=sn75799629&docId=IPC20070420145537#docIndex=19&page=3). 23 August 2005. Archived (https://web.archive.org/web/20150428011752/http://tsdr.uspto.gov/documentviewer?caseId=sn75799629&docId=IPC20070420145537#docIndex=19&page=3) from the original on 28 April 2015. Retrieved 21 September 2014. "first used the Certification Mark … as early as August 1999"
31. Doctorow, Cory (8 November 2005). "WiFi isn't short for "Wireless Fidelity" " (https://boingboing.net/2005/11/08/wifi-isnt-short-for.html). *Boing Boing*. Archived (https://web.archive.org/web/20121221132049/http://boingboing.net/2005/11/08/wifi-isnt-short-for.html) from the original on 21 December 2012. Retrieved 21 December 2012.
32. Graychase, Naomi (27 April 2007). " 'Wireless Fidelity' Debunked" (https://web.archive.org/web/20070928040415/http://www.wi-fiplanet.com/columns/article.php/3674591). *Wi-Fi Planet*. Archived from the original (http://www.wi-fiplanet.com/columns/article.php/3674591) on 28 September 2007. Retrieved 31 August 2007.
33. "Securing Wi-Fi Wireless Networks with Today's Technologies" (http://www.netsense.info/downloads/Whitepaper_Wi-Fi_Networks2-6-03.pdf) (PDF). Wi-Fi Alliance. 6 February 2003. Archived (https://web.archive.org/web/20150626100202/http://www.netsense.info/downloads/Whitepaper_Wi-Fi_Networks2-6-03.pdf) (PDF) from the original on 26 June 2015. Retrieved 25 June 2015.
34. Corrigan, Hope (30 December 2022). "I just found out what Wi-Fi means and it's sending me" (https://www.pcgamer.com/i-just-found-out-what-wi-fi-means-and-its-sending-me/). *PC Gamer*. Retrieved 2 May 2025.
35. "WPA Deployment Guidelines for Public Access Wi-Fi Networks" (https://web.archive.org/web/20070306081352/http://www.wi-fi.org/files/wp_6_WPA%20Deployment%20for%20Public%20Access_10-28-04.pdf) (PDF). Wi-Fi Alliance. 28 October 2004. Archived from the original (https://www.wi-fi.org/files/wp_6_WPA%20Deployment%20for%20Public%20Access_10-28-04.pdf) (PDF) on 6 March 2007. Retrieved 30 November 2009.
36. *HTC S710 User Manual*. High Tech Computer Corp. 2006. p. 2. "Wi-Fi is a registered trademark of the Wireless Fidelity Alliance, Inc."
37. Varma, Vijay K. "Wireless Fidelity – WiFi" (https://web.archive.org/web/20170829232140/http://www.ieee.org/about/technologies/emerging/wifi.pdf) (PDF). *Institute of Electrical and Electronics Engineers (IEEE)*. Archived from the original (https://www.ieee.org/about/technologies/emerging/wifi.pdf) (PDF) on 29 August 2017. Retrieved 16 October 2016. (originally published 2006)
38. Aime, Marco Domenico; Calandriello, Giorgio; Lioy, Antonio (January 2007). "Dependability in Wireless Networks: Can We Rely on WiFi?" (http://porto.polito.it/1515418/). *IEEE Security & Privacy*. **5** (1): 23–29. Bibcode:2007ISPri...5a..23D (https://ui.adsabs.harvard.edu/abs/2007ISPri...5a..23D). doi:10.1109/MSP.2007.4 (https://doi.org/10.1109%2FMSP.2007.4).
39. "You May Feel Silly When You Find Out What Wi-Fi Actually Stands For" (https://www.huffpost.com/entry/why-called-wi-fi_l_5cace3f7e4b01bf960065841). *HuffPost*. 15 April 2019. Retrieved 19 June 2024.
40. "IEEE 802.11-2007: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications" (https://web.archive.org/web/20070418182559/http://standards.ieee.org/getieee802/802.11.html). IEEE Standards Association. 8 March 2007. Archived from the original (https://standards.ieee.org/getieee802/802.11.html) on 18 April 2007.
41. "Wi-Fi Alliance: Programs" (https://www.wi-fi.org/certification_programs.php). www.wi-fi.org. Archived (https://web.archive.org/web/20091125024029/http://www.wi-fi.org/certification_programs.php) from the original on 25 November 2009. Retrieved 22 October 2009.
42. "Wi-Fi Alliance" (http://whatis.techtarget.com/definition/Wi-Fi-Alliance). TechTarget. Archived (https://web.archive.org/web/20160422151727/http://whatis.techtarget.com/definition/Wi-Fi-Alliance) from the original on 22 April 2016. Retrieved 8 April 2016.

43. "Wi-Fi Alliance statement regarding "Super Wi-Fi" " (https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-statement-regarding-super-wi-fi). Wi-Fi Alliance. Archived (https://web.archive.org/web/20160409001236/http://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-statement-regarding-super-wi-fi) from the original on 9 April 2016. Retrieved 8 April 2016.
44. Sascha Segan (27 January 2012). " 'Super Wi-Fi': Super, But Not Wi-Fi" (https://www.pcmag.com/article2/0,2817,2399447,00.asp). *PC Magazine*. Archived (https://web.archive.org/web/20160420010038/http://www.pcmag.com/article2/0,2817,2399447,00.asp) from the original on 20 April 2016. Retrieved 8 April 2016.
45. "The Evolution of Wi-Fi Technology and Standards" (https://standards.ieee.org/beyond-standards/the-evolution-of-wi-fi-technology-and-standards/). IEEE. 16 May 2023. Retrieved 7 August 2025.
46. "Generational Wi-Fi® User Guide" (https://www.wi-fi.org/file/generational-wi-fi-user-guide). *Wi-Fi Alliance*. Wi-Fi Alliance. April 2023. Retrieved 2 May 2026.
47. Karamyshev, Anton; Levitsky, Ilya; Bankov, Dmitry; Khorov, Evgeny (6 October 2025). "A Tutorial on Wi-Fi 8: The Journey to Ultra High Reliability" (https://doi.org/10.1134%2FS003294602502005X). *Problems of Information Transmission*. **61** (2): 164–210. doi:10.1134/S003294602502005X (https://doi.org/10.1134%2FS003294602502005X).
48. Giordano, Lorenzo; Geraci, Giovanni; Carrascosa, Marc; Bellalta, Boris (21 November 2023). "What Will Wi-Fi 8 Be? A Primer on IEEE 802.11bn Ultra High Reliability". *IEEE Communications Magazine*. **62** (8): 126. arXiv:2303.10442 (https://arxiv.org/abs/2303.10442). Bibcode:2024IComM..62h.126G (https://ui.adsabs.harvard.edu/abs/2024IComM..62h.126G). doi:10.1109/MCOM.001.2300728 (https://doi.org/10.1109%2FMCOM.001.2300728).
49. Fang, Bradley; Roger, Michael (2025). "Road Rules for Radio: Why Your Wi-Fi Got Better". arXiv:2512.23901 (https://arxiv.org/abs/2512.23901) [cs.NI (https://arxiv.org/archive/cs.NI)].
50. "Wi-Fi Alliance Introduces Wi-Fi 6" (https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-6). Wi-Fi Alliance. 3 October 2018. Archived (https://web.archive.org/web/20190403165940/https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-6) from the original on 3 April 2019. Retrieved 24 October 2019.
51. "Generational Wi-Fi User Guide" (https://www.wi-fi.org/file/generational-wi-fi-user-guide) (PDF). *www.wi-fi.org*. October 2018. Archived (https://web.archive.org/web/20220130074844/https://www.wi-fi.org/downloads-public/Generational_Wi-Fi_User_Guide_20181003.pdf/35678) from the original on 30 January 2022. Retrieved 16 March 2021.
52. Smit, Deb (5 October 2011). "How Wi-Fi got its start on the campus of CMU, a true story" (https://web.archive.org/web/20111007191316/http://www.popcitymedia.com/innovationnews/wifi100511.aspx). *Pop City*. Archived from the original (http://popcitymedia.com/innovationnews/wifi100511.aspx) on 7 October 2011. Retrieved 6 October 2011.
53. "Wireless Andrew: Creating the World's First Wireless Campus" (https://web.archive.org/web/20110901202026/http://www.cmu.edu/corporate/news/2007/features/wireless_andrew.shtml). Carnegie Mellon University. 2007. Archived from the original (http://www.cmu.edu/corporate/news/2007/features/wireless_andrew.shtml) on 1 September 2011. Retrieved 6 October 2011.
54. Lemstra, Wolter; Hayes, Vic; Groenewegen, John (2010). *The Innovation Journey of Wi-Fi: The Road to Global Success* (https://books.google.com/books?id=-OMoL5Irm08C&pg=PA121). Cambridge University Press. p. 121. ISBN 978-0-521-19971-1. Archived (https://web.archive.org/web/20121112175135/http://books.google.com/books?id=-OMoL5Irm08C&pg=PA121) from the original on 12 November 2012. Retrieved 6 October 2011.
55. Verma, Veruna (20 August 2006). "Say Hello to India's First Wirefree City" (https://www.telegraphindia.com/opinion/say-hello-to-india-s-first-wirefree-city/cid/1025843). *The Telegraph*. Archived (https://web.archive.org/web/20120120071302/http://www.telegraphindia.com/1060820/asp/opinion/story_6632793.asp) from the original on 20 January 2012.
56. "Sunnyvale Uses Metro Fi" (https://web.archive.org/web/20150722113251/http://www.besttech.com.tr/urun/bq100-gsm-role-kontrol/) (in Turkish). besttech.com.tr. Archived from the original (http://www.besttech.com.tr/urun/bq100-gsm-role-kontrol/) on 22 July 2015.

57. Alexander, Steve; Brandt, Steve (5 December 2010). "Minneapolis moves ahead with wireless" (https://web.archive.org/web/20101209140054/http://www.startribune.com/business/111286134.html). *The Star Tribune*. Archived from the original (http://www.startribune.com/business/111286134.html) on 9 December 2010.
58. "London-wide wi-fi by 2012 pledge" (https://news.bbc.co.uk/1/hi/england/london/8692103.stm). *BBC News*. 19 May 2010. Archived (https://web.archive.org/web/20100522121915/http://news.bbc.co.uk/2/hi/uk_news/england/london/8692103.stm) from the original on 22 May 2010. Retrieved 19 May 2010.
59. Bsu, Indrajit (14 May 2007). "City of London Fires Up Europe's Most Advanced Wi-Fi Network" (https://web.archive.org/web/20080907195450/http://www.govtech.com/dc/118717). *Digital Communities*. Archived from the original (http://www.govtech.com/dc/118717) on 7 September 2008. Retrieved 14 May 2007.
60. Wearden, Graeme (18 April 2005). "London gets a mile of free Wi-Fi" (https://www.zdnet.com/home-and-office/networking/london-gets-a-mile-of-free-wi-fi/). *ZDNet*. Archived (https://web.archive.org/web/20151107174238/http://www.zdnet.com/article/london-gets-a-mile-of-free-wi-fi/) from the original on 7 November 2015. Retrieved 6 January 2015.
61. Chowdhry, Amit (19 November 2014). "Pay Phones In NYC To Be Replaced With Up To 10,000 Free Wi-Fi Kiosks Next Year" (https://www.forbes.com/sites/amitchowdhry/2014/11/19/linknyc-free-wifi/#11c29eb27028). *Forbes*. Archived (https://web.archive.org/web/20160922212101/http://www.forbes.com/sites/amitchowdhry/2014/11/19/linknyc-free-wifi/#11c29eb27028) from the original on 22 September 2016. Retrieved 17 September 2016.
62. Gould, Jessica (5 January 2016). "Goodbye Pay Phones, Hello LinkNYC" (https://www.wnyc.org/story/goodbye-pay-phones-hello-linknyc/). *WNYC*. Archived (https://web.archive.org/web/20160820213828/http://www.wnyc.org/story/goodbye-pay-phones-hello-linknyc/) from the original on 20 August 2016. Retrieved 26 January 2016.
63. "New York City unveils the pay phone of the future – and it does a whole lot more than make phone calls" (https://www.washingtonpost.com/news/wonk/wp/2014/11/17/new-york-city-unveils-the-payphone-of-the-future-and-it-does-a-whole-lot-more-than-make-phone-calls/). *Washington Post*. 17 November 2014. Archived (https://web.archive.org/web/20160919171319/https://www.washingtonpost.com/news/wonk/wp/2014/11/17/new-york-city-unveils-the-payphone-of-the-future-and-it-does-a-whole-lot-more-than-make-phone-calls/) from the original on 19 September 2016. Retrieved 17 September 2016.
64. "De Blasio Administration Announces Winner of Competition to Replace Payphones with Five-Borough Wi-Fi Network" (http://www1.nyc.gov/office-of-the-mayor/news/923-14/de-blasio-administration-winner-competition-replace-payphones-five-borough). *nyc.gov*. Government of New York City. 17 November 2014. Archived (https://web.archive.org/web/20180607153357/http://www1.nyc.gov/office-of-the-mayor/news/923-14/de-blasio-administration-winner-competition-replace-payphones-five-borough) from the original on 7 June 2018. Retrieved 17 November 2014.
65. Alba, Alejandro (5 January 2016). "New York to start replacing payphones with Wi-Fi kiosks" (http://www.nydailynews.com/news/national/new-york-start-replacing-payphone-wi-fi-kiosks-article-1.2485429). *New York Daily News*. Archived (https://web.archive.org/web/20170624191512/http://www.nydailynews.com/news/national/new-york-start-replacing-payphone-wi-fi-kiosks-article-1.2485429) from the original on 24 June 2017. Retrieved 26 January 2016.
66. McCormick, Rich (25 October 2016). "Link brings its free public Wi-Fi booths from New York to London" (https://www.theverge.com/2016/10/25/13401348/link-public-wi-fi-kiosk-london). *The Verge*. Archived (https://web.archive.org/web/20161226145341/http://www.theverge.com/2016/10/25/13401348/link-public-wi-fi-kiosk-london) from the original on 26 December 2016. Retrieved 25 July 2021.

67. "Seoul Moves to Provide Free City-Wide WiFi Service" (https://web.archive.org/web/20121110050549/http://blogs.voanews.com/breaking-news/2011/06/15/seoul-moves-to-provide-free-city-wide-wifi-service/). *Voice of America*. 15 June 2011. Archived from the original (https://blogs.voanews.com/breaking-news/2011/06/15/seoul-moves-to-provide-free-city-wide-wifi-service/) on 10 November 2012. Retrieved 1 April 2012.
68. Krzysztof W. Kolodziej; Johan Hjelm (19 December 2017). *Local Positioning Systems: LBS Applications and Services* (https://books.google.com/books?id=aV3LBQAAQBAJ). CRC Press. ISBN 978-1-4200-0500-4. Archived (https://web.archive.org/web/20230117221756/https://books.google.com/books?id=aV3LBQAAQBAJ) from the original on 17 January 2023. Retrieved 6 October 2019.
69. .Wang, C.; Zheng, X.; Chen, Y.; Yang, J. (September 2017). "Locating Rogue Access Point Using Fine-Grained Channel Information". *IEEE Transactions on Mobile Computing*. **16** (9): 2560–2573. Bibcode:2017ITMC...16.2560W (https://ui.adsabs.harvard.edu/abs/2017ITMC...16.2560W). doi:10.1109/TMC.2016.2629473 (https://doi.org/10.1109%2FTMC.2016.2629473).
70. "Cisco Prime Network Control System Configuration Guide, Release 1.0 - Chapter 6: Monitoring Maps [Cisco Prime Network Control System Series Appliances]" (https://www.cisco.com/c/en/us/td/docs/wireless/ncs/1-0/configuration/guide/NCS10cg/maps.html). *Cisco*. Retrieved 19 December 2020.
71. Magda Chelly; Nel Samama (September 2010). *Detecting visibility in heterogeneous simulated environments for positioning purposes* (https://hal.science/hal-01345039). IPIN 2010: International Conference on Indoor Positioning and Indoor Navigation. Hoenggerberg, Switzerland. hal-01345039.
72. Magda Chelly; Nel Samama (May 2009). *New techniques for indoor positioning, combining deterministic and estimation methods* (https://hal.science/hal-01367483/). ENC-GNSS 2009: European Navigation Conference – Global Navigation Satellite Systems. Naples, Italy. pp. 1–12. hal-01367483.
73. Forlano, Laura (8 October 2009). "WiFi Geographies: When Code Meets Place". *The Information Society*. **25** (5): 344–352. doi:10.1080/01972240903213076 (https://doi.org/10.1080%2F01972240903213076).
74. Y. Chen; H. Kobayashi (April–May 2002). "Signal strength based indoor geolocation". *Proceedings of the IEEE International Conference on Communications (ICC '02)*. Vol. 1. New York, NY, USA. pp. 436–439. doi:10.1109/ICC.2002.996891 (https://doi.org/10.1109%2FICC.2002.996891). ISBN 0-7803-7400-2.
75. Youssef, M.A.; Agrawala, A.; Udaya Shankar, A. (2003). "WLAN location determination via clustering and probability distributions". *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications, 2003. (PerCom 2003)*. pp. 143–150. doi:10.1109/PERCOM.2003.1192736 (https://doi.org/10.1109%2FPERCOM.2003.1192736). ISBN 0-7695-1893-1.
76. Youssef, Moustafa; Youssef, Adel; Rieger, Chuck; Shankar, Udaya; Agrawala, Ashok (2006). "PinPoint: An Asynchronous Time-Based Location Determination System". *Proceedings of the 4th international conference on Mobile systems, applications and services*. pp. 165–176. doi:10.1145/1134680.1134698 (https://doi.org/10.1145%2F1134680.1134698). ISBN 1-59593-195-3.
77. Danalet, Antonin; Farooq, Bilal; Bierlaire, Michel (July 2014). "A Bayesian approach to detect pedestrian destination-sequences from WiFi signatures" (https://infoscience.epfl.ch/record/199471/files/DanaletFarooqBierlaire_2014.pdf) (PDF). *Transportation Research Part C: Emerging Technologies*. **44**: 146–170. Bibcode:2014TRPC...44..146D (https://ui.adsabs.harvard.edu/abs/2014TRPC...44..146D). doi:10.1016/j.trc.2014.03.015 (https://doi.org/10.1016%2Fj.trc.2014.03.015).
78. Decker, Kris De (6 June 2017). "Comment bâtir un internet low tech" (http://journals.openedition.org/tc/8489) [How to Build a Low-tech Internet]. *Techniques & Culture* (in French). **67** (67): 216–235. doi:10.4000/tc.8489 (https://doi.org/10.4000%2Ftc.8489).

79. Hashem, Omar; Harras, Khaled A.; Youssef, Moustafa (August 2021). "Accurate indoor positioning using IEEE 802.11mc round trip time". *Pervasive and Mobile Computing*. **75** 101416. doi:10.1016/j.pmcj.2021.101416 (https://doi.org/10.1016%2Fj.pmcj.2021.101416).
80. "Newly Released IEEE 802.11az Standard Improving Wi-Fi Location Accuracy is Set to Unleash a New Wave of Innovation" (https://standards.ieee.org/beyond-standards/newly-released-ieee-802-11az-standard-improving-wi-fi-location-accuracy-is-set-to-unleash-a-new-wave-of-innovation/) (Press release). Retrieved 24 October 2023.
81. "Wi-Fi location-based services: How did we get here?" (https://blogs.arubanetworks.com/solutions/wi-fi-location-based-services-how-did-we-get-here/). 27 February 2023. Retrieved 24 October 2023.
82. Khalili, Abdullah; Soliman, Abdel-Hamid; Asaduzzaman, Md; Griffiths, Alison (March 2020). "Wi-Fi sensing: applications and challenges" (https://doi.org/10.1049%2Fjoe.2019.0790). *The Journal of Engineering*. **2020** (3): 87–97. doi:10.1049/joe.2019.0790 (https://doi.org/10.1049%2Fjoe.2019.0790).
83. Cisco Systems, Inc. White Paper Capacity, Coverage, and Deployment Considerations for IEEE 802.11g
84. Gast, Matthew S. (2013). "Chapter 4. Beamforming in 802.11ac" (https://web.archive.org/web/20170703105148/http://chimera.labs.oreilly.com/books/1234000001739/ch04.html). *802.11ac: A Survival Guide*. O'Reilly Atlas. Archived from the original (http://chimera.labs.oreilly.com/books/1234000001739/ch04.html) on 3 July 2017. Retrieved 17 April 2014.
85. "Why can't WiFi work as full duplex while 3G and 4G can" (https://community.meraki.com/t5/Wireless-LAN/Why-can-t-WiFi-work-as-full-duplex-while-3G-and-4G-can/m-p/74017#M11290). *Meraki Community*. 23 January 2020. Archived (https://web.archive.org/web/20211017103935/https://community.meraki.com/t5/Wireless-LAN/Why-can-t-WiFi-work-as-full-duplex-while-3G-and-4G-can/m-p/74017#M11290) from the original on 17 October 2021. Retrieved 19 September 2020.
86. Badman, Lee (26 August 2019). "Bad Info Is Nothing New for WLAN- Don't Believe "Full Duplex" in Wi-Fi 6" (https://www.toolbox.com/tech/it-strategy/blogs/bad-info-is-nothing-new-for-wlan-dont-believe-full-duplex-in-wi-fi-6-082619/). *Toolbox*. Archived (https://web.archive.org/web/20211119071542/https://www.toolbox.com/tech/it-strategy/blogs/bad-info-is-nothing-new-for-wlan-dont-believe-full-duplex-in-wi-fi-6-082619/) from the original on 19 November 2021. Retrieved 19 September 2020.
87. "Federal Standard 1037C" (https://web.archive.org/web/20090302235918/http://www.its.bldrdoc.gov/fs-1037/fs-1037c.htm). *Institute for Telecommunication Sciences*. 7 August 1996. Archived from the original (http://www.its.bldrdoc.gov/fs-1037/fs-1037c.htm) on 2 March 2009. Retrieved 9 September 2012.
88. "ATIS Telecom Glossary 2007" (https://web.archive.org/web/20080302071329/http://www.atis.org/tg2k/). *Alliance for Telecommunications Industry Solutions*. ATIS-0100523.2007. Archived from the original (http://www.atis.org/tg2k/) on 2 March 2008. Retrieved 9 September 2012.
89. "Wi-Fi Channels, Frequencies, Bands & Bandwidths" (https://www.radio-electronics.com/info/wireless/wi-fi/80211-channels-number-frequencies-bandwidth.php). *Electronics Notes*. Archived (https://web.archive.org/web/20180216081725/https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/channels-frequencies-bands-bandwidth.php) from the original on 16 February 2018. Retrieved 18 August 2018.
90. *IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. doi:10.1109/IEEESTD.2016.7786995 (https://doi.org/10.1109%2FIEEESTD.2016.7786995). ISBN 978-1-5044-3645-8.

91. "802.11 WiFi Standards Explained" (https://www.lifewire.com/wireless-standards-802-11a-802-11b-g-n-and-802-11ac-816553). *Lifewire*. Archived (https://web.archive.org/web/20181212063416/https://www.lifewire.com/wireless-standards-802-11a-802-11b-g-n-and-802-11ac-816553) from the original on 12 December 2018. Retrieved 18 August 2018.
92. "USB 3.0 Radio Frequency Interference Impact on 2.4 GHz Wireless Devices" (http://www.usb.org/developers/docs/whitepapers/327216.pdf) (PDF). *USB.org*. USB Implementers Forum. April 2012. Retrieved 14 October 2019.
93. "Why Everything Wireless Is 2.4 GHz" (https://www.wired.com/2010/09/wireless-explainer/). *WIRED*. Archived (https://web.archive.org/web/20180726115300/https://www.wired.com/2010/09/wireless-explainer/) from the original on 26 July 2018. Retrieved 18 August 2018.
94. "802.11n Data Rates Dependability and scalability" (https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1250-series/design_guide_c07-693245.html#_Toc309331071). Cisco. Archived (https://web.archive.org/web/20170705034144/http://www.cisco.com/c/en/us/products/collateral/wireless/Aironet-1250-series/design_guide_c07-693245.html#_Toc309331071) from the original on 5 July 2017. Retrieved 20 November 2017.
95. "3.1.1 Packet format" (https://web.archive.org/web/20141021020414/http://standards.ieee.org/getieee802/download/802.3-2012_section1.pdf) (PDF). *IEEE Standard for Ethernet, 802.3-2012 – section one*. 28 December 2012. p. 53. Archived from the original (http://standards.ieee.org/getieee802/download/802.3-2012_section1.pdf) (PDF) on 21 October 2014. Retrieved 6 July 2014.
96. Stobing, Chris (14 February 2024). "What Does WiFi Stand For? | WiFi Meaning & How It Works" (https://www.gadgetreview.com/what-does-wifi-stand-for). *GadgetReview*. Retrieved 21 October 2025.
97. Geier, Jim (6 December 2001). *Overview of the IEEE 802.11 Standard* (http://www.informit.com/articles/article.aspx?p=24411&seqNum=7). InformIT. Archived (https://web.archive.org/web/20160420043213/http://www.informit.com/articles/article.aspx?p=24411&seqNum=7) from the original on 20 April 2016. Retrieved 8 April 2016.
98. US 5987011 (https://worldwide.espacenet.com/textdoc?DB=EPODOC&IDX=US5987011), Toh, Chai Keong, "Routing Method for Ad-Hoc Mobile Networks", published 16 November 1999
99. "Mobile Computing Magazines and Print Publications" (http://www.mobileinfo.com/education/magazines.htm). *www.mobileinfo.com*. Archived (https://web.archive.org/web/20160426220723/http://www.mobileinfo.com/education/magazines.htm) from the original on 26 April 2016. Retrieved 19 December 2017.
100. Toh, C.-K; Delwar, M.; Allen, D. (7 August 2002). "Evaluating the Communication Performance of an Ad Hoc Mobile Network". *IEEE Transactions on Wireless Communications*. **1** (3): 402–414. doi:10.1109/TWC.2002.800539 (https://doi.org/10.1109%2FTWC.2002.800539).
101. Toh, C.-K.; Chen, Richard; Delwar, Minar; Allen, Donald (December 2000). "Experimenting with an Ad Hoc wireless network on campus: insights and experiences". *ACM SIGMETRICS Performance Evaluation Review*. **28** (3): 21–29. doi:10.1145/377616.377622 (https://doi.org/10.1145%2F377616.377622).
102. Subash (24 January 2011). "Wireless Home Networking with Virtual WiFi Hotspot" (https://techsansar.com/internetworking/wireless-home-networking-virtual-wifi-hotspot/). *Techsansar*. Archived (https://web.archive.org/web/20110830150439/http://techsansar.com/internetworking/wireless-home-networking-virtual-wifi-hotspot-2946/) from the original on 30 August 2011. Retrieved 14 October 2011.
103. Cox, John (14 October 2009). "Wi-Fi Direct allows device-to-device links" (https://web.archive.org/web/20091023052219/http://www.networkworld.com/news/2009/101409-wi-fi-direct.html?hpg1=bn). *Network World*. Archived from the original (http://www.networkworld.com/news/2009/101409-wi-fi-direct.html?hpg1=bn) on 23 October 2009.

104. "Wi-Fi gets personal: Groundbreaking Wi-Fi Direct launches today" (https://web.archive.org/web/20150626120701/http://www.wi-fi.org/news-events/newsroom/wi-fi-gets-personal-groundbreaking-wi-fi-direct-launches-today) (Press release). Wi-Fi Alliance. 25 October 2010. Archived from the original (https://www.wi-fi.org/news-events/newsroom/wi-fi-gets-personal-groundbreaking-wi-fi-direct-launches-today) on 26 June 2015. Retrieved 25 June 2015.
105. "What is Wi-Fi Certified TDLS?" (https://web.archive.org/web/20141108145755/http://www.wi-fi.org/knowledge-center/faq/what-is-wi-fi-certified-tdls). Wi-Fi Alliance. Archived from the original (https://www.wi-fi.org/knowledge-center/faq/what-is-wi-fi-certified-tdls) on 8 November 2014.
106. Edney, Jon (2004), "What is an ESS?" (http://www.ieee802.org/21/doctree/2004_Meeting_Docs/2004-07_meeting_docs/21-04-0105-00-0000-what_ess.ppt), *IEEE 802 LAN/MAN Standards Committee Meeting, July 2004*, Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, p. 8
107. Mohsin Beg (3 December 2021). "Fix WiFi Connected But No Internet Access On Windows 11/10/8/7" (https://newscutzy.com/windows/fix-wifi-connected-but-no-internet-access/). newscutzy.com. Archived (https://web.archive.org/web/20210624202339/https://newscutzy.com/windows/fix-wifi-connected-but-no-internet-access/) from the original on 24 June 2021. Retrieved 25 June 2020.
108. Tjensvold, Jan Magne (18 September 2007). "Comparison of the IEEE 802.11, 802.15.1,802.15.4, and 802.15.6 wireless standards" (https://janmagnet.files.wordpress.com/2008/07/comparison-ieee-802-standards.pdf) (PDF). Archived (https://web.archive.org/web/20130720054917/http://janmagnet.files.wordpress.com/2008/07/comparison-ieee-802-standards.pdf) (PDF) from the original on 20 July 2013. Retrieved 26 April 2013. section 1.2 (scope)
109. "Somebody explain dBi – Wireless Networking" (http://www.dslreports.com/forum/r15405199-Somebody-explain-dBi). *DSL Reports Forums*. Archived (https://web.archive.org/web/20140809101928/http://www.dslreports.com/forum/r15405199-Somebody-explain-dBi) from the original on 9 August 2014.
110. "802.11n Delivers Better Range" (https://web.archive.org/web/20151108080354/http://www.wi-fiplanet.com/tutorials/article.php/3680781). *Wi-Fi Planet*. 31 May 2007. Archived from the original (http://www.wi-fiplanet.com/tutorials/article.php/3680781) on 8 November 2015.
111. "WiFi Mapping Software:Footprint" (http://www.alyrica.net/node/20). Alyrica Networks. Archived (https://web.archive.org/web/20090502175411/http://www.alyrica.net/node/20) from the original on 2 May 2009. Retrieved 27 April 2008.
112. Kanellos, Michael (18 June 2007). "Ermanno Pietrosemoli has set a new record for the longest communication Wi-Fi link" (https://interred.wordpress.com/2007/06/18/ermanno-pietrosemoli-has-set-a-new-record-for-the-longest-communication-wi-fi-link/). Archived (https://web.archive.org/web/20080321104324/http://interred.wordpress.com/2007/06/18/ermanno-pietrosemoli-has-set-a-new-record-for-the-longest-communication-wi-fi-link/) from the original on 21 March 2008. Retrieved 10 March 2008.
113. Pietrosemoli, Ermanno (18 May 2007). "Long Distance WiFi Trial" (https://yourgadgetgeek.com/media_file/long_distance_wiFi_trial.pdf) (PDF). Archived (https://web.archive.org/web/20160305165645/http://www.wifiadvies.be/wp-content/uploads/2015/11/200705_long_distance_wiFi_trial.pdf) (PDF) from the original on 5 March 2016. Retrieved 10 March 2008.
114. Chakraborty, Sandip; Nandi, Sukumar; Chattopadhyay, Subhrendu (February 2016). "Alleviating Hidden and Exposed Nodes in High-Throughput Wireless Mesh Networks". *IEEE Transactions on Wireless Communications*. **15** (2): 928–937. Bibcode:2016ITWC...15..928C (https://ui.adsabs.harvard.edu/abs/2016ITWC...15..928C). doi:10.1109/TWC.2015.2480398 (https://doi.org/10.1109%2FTWC.2015.2480398).

115. Villegas, Eduard Garcia; Lopez-Aguilera, Elena; Vidal, Rafael; Paradells, Josep (2007). "Effect of adjacent-channel interference in IEEE 802.11 WLANs". *2007 2nd International Conference on Cognitive Radio Oriented Wireless Networks and Communications*. pp. 118–125. doi:10.1109/CROWNCOM.2007.4549783 (https://doi.org/10.1109%2FCROWNCOM.2007.4549783). hdl:2117/1234 (https://hdl.handle.net/2117%2F1234). ISBN 978-1-4244-0814-6.
116. den Hartog, F., Raschella, A., Bouhafs, F., Kempker, P., Boltjes, B., & Seyedebrahimi, M. (November 2017). A Pathway to solving the Wi-Fi Tragedy of the Commons in apartment blocks (http://unsworks.unsw.edu.au/fapi/datastream/unsworks:50254/bin458a10d9-f568-479c-a9b5-5c185ef64e78?view=true) Archived (https://web.archive.org/web/20200713111300/http://unsworks.unsw.edu.au/fapi/datastream/unsworks:50254/bin458a10d9-f568-479c-a9b5-5c185ef64e78?view=true) 13 July 2020 at the Wayback Machine. In 2017 27th International Telecommunication Networks and Applications Conference (ITNAC) (pp. 1–6). IEEE.
117. Wilson, Tracy V. (17 April 2006). "How Municipal WiFi Works" (https://computer.howstuffworks.com/municipal-wifi.htm). *HowStuffWorks*. Archived (https://web.archive.org/web/20080223120947/http://computer.howstuffworks.com/municipal-wifi.htm) from the original on 23 February 2008. Retrieved 12 March 2008.
118. Caravan, Delia (12 September 2014). "6 Easy Steps To Protect Your Baby Monitor From Hackers" (https://web.archive.org/web/20141018042051/https://www.monitorshq.com/6-easy-steps-to-protect-your-baby-monitor-from-hackers/). *Baby Monitor Reviews HQ*. Archived from the original (https://www.monitorshq.com/6-easy-steps-to-protect-your-baby-monitor-from-hackers/) on 18 October 2014. Retrieved 12 September 2014.
119. Brown, Bob (10 March 2016). "Wi-Fi hotspot blocking persists despite FCC crackdown" (https://www.networkworld.com/article/949170/wi-fi-hotspot-blocking-persists-despite-fcc-crackdown.html). *Network World*. Archived (https://web.archive.org/web/20190227033935/https://www.networkworld.com/article/3042454/wi-fi-hotspot-blocking-persists-despite-fcc-crackdown.html) from the original on 27 February 2019.
120. *Towards Energy-Awareness in Managing Wireless LAN Applications* (https://www.researchgate.net/publication/241631429). IEEE/IFIP Network Operations and Management Symposium. IEEE/IFIP NOMS. 2012. doi:10.1109/NOMS.2012.6211930 (https://doi.org/10.1109%2FNOMS.2012.6211930). Retrieved 21 October 2025.
121. *Application Level Energy and Performance Measurements in a Wireless LAN* (https://www.researchgate.net/publication/224264522). 2011 IEEE/ACM International Conference on Green Computing and Communications. doi:10.1109/GreenCom.2011.26 (https://doi.org/10.1109%2FGreenCom.2011.26). Retrieved 21 October 2025.
122. Veendrick, Harry J. M. (2017). *Nanometer CMOS ICs: From Basics to ASICs* (https://books.google.com/books?id=Lv_EDgAAQBAJ&pg=PA243). Springer. p. 243. ISBN 9783319475974. Archived (https://web.archive.org/web/20230117221755/https://books.google.com/books?id=Lv_EDgAAQBAJ&pg=PA243) from the original on 17 January 2023. Retrieved 26 October 2019.
123. "Free WiFi Analyzer-Best Channel Analyzer Apps For Wireless Networks" (https://web.archive.org/web/20170808000116/https://www.thedigitalworm.com/free-wifi-analyzer-apps/). *The Digital Worm*. 8 June 2017. Archived from the original on 8 August 2017.
124. "Apple.com Airport Utility Product Page" (https://web.archive.org/web/20110608183330/http://www.apple.com/airportextreme/features/utility.html). Apple, Inc. Archived from the original on 8 June 2011. Retrieved 14 June 2011.
125. "GainSpan low-power, embedded Wi-Fi" (https://web.archive.org/web/20100630050952/http://www.gainspan.com/technology/technology_overview.php). www.gainspan.com. Archived from the original (http://www.gainspan.com/technology/technology_overview.php) on 30 June 2010. Retrieved 17 June 2017.

126. "Quatech Rolls Out Airborne Embedded 802.11 Radio for M2M Market" (http://edageek.com/2008/04/18/embedded-wifi-radio/). Archived (https://web.archive.org/web/20080428103306/http://edageek.com/2008/04/18/embedded-wifi-radio/) from the original on 28 April 2008. Retrieved 29 April 2008.
127. "CIE article on embedded Wi-Fi for M2M applications" (https://web.archive.org/web/20150418040305/http://wifiscan.fr/research/article_19742.htm). Archived from the original (http://wifiscan.fr/research/article_19742.htm) on 18 April 2015. Retrieved 28 November 2014.
128. "Wifi Connectivity Explained | MAC Installations & Consulting" (https://web.archive.org/web/20200505091852/https://www.macinstallations.com/wifi-connectivity-explained/). Archived from the original (https://www.macinstallations.com/wifi-connectivity-explained/) on 5 May 2020. Retrieved 9 February 2020.
129. Jensen, Joe (26 October 2007). "802.11 X Wireless Network in a Business Environment – Pros and Cons" (https://web.archive.org/web/20080305075900/http://networkbits.net/wireless-printing/80211-g-pros-cons-of-a-wireless-network-in-a-business-environment/). *Networkbits*. Archived from the original on 5 March 2008. Retrieved 8 April 2008.
130. Higgs, Larry (1 July 2013). "Free Wi-Fi? User beware: Open connections to Internet are full of security dangers, hackers, ID thieves" (http://www.app.com/article/20130701/NJNEWS/307010010/Free-Wi-Fi-User-beware-Open-connections-Internet-full-security-dangers). *Asbury Park Press*.
131. Gittleson, Kim (28 March 2014). "Data-stealing Snoopy drone unveiled at Black Hat" (https://www.bbc.com/news/technology-26762198). *BBC News*. Archived (https://web.archive.org/web/20140330062159/http://www.bbc.co.uk/news/technology-26762198) from the original on 30 March 2014. Retrieved 29 March 2014.
132. Bernstein, Daniel J. (2002). "DNS forgery" (http://cr.yp.to/djbdns/forgery.html). Archived (https://web.archive.org/web/20090727073417/http://cr.yp.to/djbdns/forgery.html) from the original on 27 July 2009. Retrieved 24 March 2010. "An attacker with access to your network can easily forge responses to your computer's DNS requests."
133. Mateti, Prabhaker (2005). "Hacking Techniques in Wireless Networks" (http://www.cs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.htm#_Toc77524658). Dayton, Ohio: Wright State University Department of Computer Science and Engineering. Archived (https://web.archive.org/web/20100305180937/http://www.cs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.htm#_Toc77524658) from the original on 5 March 2010. Retrieved 28 February 2010.
134. "AirSnort" (http://www.wirelessve.org/entries/show/WVE-2005-0020#selection-373.1-376.0). *Wireless Vulnerabilities & Exploits*.
135. "WPA2 Security Now Mandatory for Wi-Fi CERTIFIED Products" (https://web.archive.org/web/20110807093143/http://www.wi-fi.org/news_articles.php?f=media_news&news_id=16). *Wi-Fi Alliance*. 13 March 2006. Archived from the original (https://www.wi-fi.org/news_articles.php?f=media_news&news_id=16) on 7 August 2011.
136. Vanhoef, Mathy (2017). "Key Reinstallation Attacks: Breaking WPA2 by forcing nonce reuse" (https://www.krackattacks.com/). Archived (https://web.archive.org/web/20171022022042/https://www.krackattacks.com/) from the original on 22 October 2017. Retrieved 21 October 2017.
137. Goodin, Dan (16 October 2017). "Serious flaw in WPA2 protocol lets attackers intercept passwords and much more" (https://arstechnica.com/information-technology/2017/10/severe-flaw-in-wpa2-protocol-leaves-wi-fi-traffic-open-to-eavesdropping/). *Ars Technica*. Archived (https://web.archive.org/web/20171021121658/https://arstechnica.com/information-technology/2017/10/severe-flaw-in-wpa2-protocol-leaves-wi-fi-traffic-open-to-eavesdropping/) from the original on 21 October 2017. Retrieved 21 October 2017.
138. "CERT/CC Vulnerability Note VU#723755" (http://www.kb.cert.org/vuls/id/723755). Archived (https://web.archive.org/web/20120103152902/http://www.kb.cert.org/vuls/id/723755) from the original on 3 January 2012. Retrieved 1 January 2012. US CERT Vulnerability Note VU#723755

139. "Tips for Using Public Wi-Fi Networks" (https://web.archive.org/web/20190809122844/https://www.consumer.ftc.gov/articles/0014-tips-using-public-wi-fi-networks#protect). *Federal Trade Commission – Consumer Information*. Federal Trade Commission. March 2014. Archived from the original (https://www.consumer.ftc.gov/articles/0014-tips-using-public-wi-fi-networks#protect) on 9 August 2019. Retrieved 8 August 2019.
140. "Share your Wi-Fi SSID & Password using a QR Code" (http://www.technostarry.com/share-wi-fi-details-using-qr-code/). 19 July 2015. Archived (https://web.archive.org/web/20230112193217/http://www.technostarry.com/share-wi-fi-details-using-qr-code/) from the original on 12 January 2023. Retrieved 28 July 2021.
141. "zxing documentation: barcode contents" (https://github.com/zxing/zxing/wiki/Barcode-Contents). *GitHub*. zxing. Archived (https://web.archive.org/web/20160215201205/https://github.com/zxing/zxing/wiki/Barcode-Contents) from the original on 15 February 2016. Retrieved 28 July 2021.
142. Thubron, Rob (9 January 2018). "WPA3 protocol will make public Wi-Fi hotspots a lot more secure" (https://www.techspot.com/news/72656-wpa3-protocol-make-public-wi-fi-hotspots-lot.html). *Techspot*. Archived (https://web.archive.org/web/20181116023123/https://www.techspot.com/news/72656-wpa3-protocol-make-public-wi-fi-hotspots-lot.html) from the original on 16 November 2018.
143. Kastrenakes, Jacob (26 June 2018). "Wi-Fi security is starting to get its biggest upgrade in over a decade" (https://www.theverge.com/circuitbreaker/2018/6/26/17501594/wpa3-wifi-security-certification). *The Verge*. Archived (https://web.archive.org/web/20190220012909/https://www.theverge.com/circuitbreaker/2018/6/26/17501594/wpa3-wifi-security-certification) from the original on 20 February 2019. Retrieved 26 June 2018.
144. "NoCat's goal is to bring you Infinite Bandwidth Everywhere for Free" (https://web.archive.org/web/20111022034826/http://nocat.net/). *NoCat.net*. Archived from the original (http://nocat.net/) on 22 October 2011. Retrieved 14 October 2011.
145. Jones, Matt (24 June 2002). "Let's Warchalk" (https://web.archive.org/web/20080705034313/http://www.blackbeltjones.com/warchalking/warchalking0_9.pdf) (PDF). Archived from the original (http://www.blackbeltjones.com/warchalking/warchalking0_9.pdf) (PDF) on 5 July 2008. Retrieved 9 October 2008.
146. "Digest of Education Statistics, 2017" (https://nces.ed.gov/programs/digest/d17/tables/dt17_702.60.asp). *nces.ed.gov*. Archived (https://web.archive.org/web/20200514043300/https://nces.ed.gov/programs/digest/d17/tables/dt17_702.60.asp) from the original on 14 May 2020. Retrieved 8 May 2020.
147. "Wi-Fi: How Broadband Households Experience the Internet | NCTA – The Internet & Television Association" (http://www.ncta.com/whats-new/wi-fi-how-broadband-households-experience-the-internet). *www.ncta.com*. 6 April 2018. Archived (https://web.archive.org/web/20200512044128/https://www.ncta.com/whats-new/wi-fi-how-broadband-households-experience-the-internet) from the original on 12 May 2020. Retrieved 8 May 2020.
148. "Electromagnetic fields and public health – Base stations and wireless technologies" (https://web.archive.org/web/20160522225458/http://www.who.int/mediacentre/factsheets/fs304/en/). World Health Organization. 2006. Archived from the original (https://www.who.int/mediacentre/factsheets/fs304/en/) on 22 May 2016. Retrieved 28 May 2016.
149. "IARC Classifies Radiofrequency Electromagnetic Fields as Possibly Carcinogenic to Humans" (https://www.iarc.fr/wp-content/uploads/2018/07/pr208_E.pdf) (PDF). International Agency for Research on Cancer. 31 May 2011. Archived (https://web.archive.org/web/20120404203349/http://www.iarc.fr/en/media-centre/pr/2011/pdfs/pr208_E.pdf) (PDF) from the original on 4 April 2012. Retrieved 28 May 2016.
150. "Electromagnetic Fields and Public Health: Mobile Phones" (https://web.archive.org/web/20160525183100/http://www.who.int/mediacentre/factsheets/fs193/en/). World Health Organization. October 2014. Archived from the original (https://www.who.int/mediacentre/factsheets/fs193/en) on 25 May 2016. Retrieved 28 May 2016.

151. "Q&A: Wi-fi health concerns" (https://news.bbc.co.uk/2/hi/technology/6677051.stm). *BBC News*. 21 May 2007. Archived (https://web.archive.org/web/20160421152005/http://news.bbc.co.uk/2/hi/technology/6677051.stm) from the original on 21 April 2016. Retrieved 28 May 2016.
152. Rubin, G James; Munshi, Jayati Das; Wessely, Simon (March 2005). "Electromagnetic Hypersensitivity: A Systematic Review of Provocation Studies". *Psychosomatic Medicine*. **67** (2): 224–232. doi:10.1097/01.psy.0000155664.13300.64 (https://doi.org/10.1097%2F01.psy.0000155664.13300.64). PMID 15784787 (https://pubmed.ncbi.nlm.nih.gov/15784787).

Further reading

- The WNDW Authors (2013). Butler, Jane (ed.). *Wireless Networking in the Developing World* (Third ed.). CreateSpace Independent Publishing Platform. ISBN 978-1-4840-3935-9.

External links

- Official website (https://www.wi-fi.org//)
- wiisfi.com – Understanding Wi-Fi 4/5/6/6E/7/8 (802.11 n/ac/ax/be/bn) (https://www.wiisfi.com/)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Wi-Fi&oldid=1363031309"